Superservicios
Superintendencia de Servicios Públicos Domiciliarios

DNP Departamento Nacional de Planeación

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MEMORANDO
20181400071833

GD-F-010 V.10

Bogotá D.C., 27/06/2018

PARA **Dra. RUTTY PAOLA ORTIZ JARA**
Superintendente

DE **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO Informe final Auditoría Interna de Gestión 2018 Proceso Gestión Tecnologías De Información - Desarrollo de Soluciones Informáticas, Sistema Único de Información y Gestión y Operación de la Infraestructura Tecnológica.

Respetada doctora:

La Oficina de Control Interno dando cumplimiento al Programa Anual de Auditorias de Gestión para la vigencia 2018 y, con el fin de valorar en forma pertinente el desempeño de los procesos y la eficacia y efectividad de los controles y del Sistema de Control Interno, ejecutó la auditoria interna de gestión al Proceso de Gestión Tecnologías De Información - Desarrollo de Soluciones Informáticas, Sistema Único de Información y Gestión y Operación de la Infraestructura Tecnológica, obteniendo como resultado el informe final de auditoria, el cual remitimos para su conocimiento.

Como resultado de dicha auditoría se generaron veintiún (21) observaciones, por tal motivo el líder del proceso deberá contar con la asesoría de la Oficina de Planeación en la formulación de acciones de mejora, de conformidad con los lineamientos establecidos en el procedimiento acciones correctivas, preventivas y de mejora - MC-P-001, en un plazo no mayor a 15 días hábiles.

La Oficina de Control Interno cumpliendo el ciclo de la presente auditoría, continuará con su labor de seguimiento y asesoría permanente, propendiendo por el mejoramiento continuo en los procesos, lo que redundará en una gestión institucional exitosa.

Cordialmente,

HERRERA.

MYRIAM HERRERA DURÁN
Anexo: Informe final de auditoría de gestión
Copia: José Alfredo Ruiz Peralta – Oficina de Informática
Lida Constanza Cubillos – Oficina Asesora de Planeación
Proyectó: Luis Ernesto Vargas - Oficina de Control Interno

Superservicios
Superintendencia de Servicios Públicos Domiciliarios

INFORME AUDITORIAS INTERNAS DE GESTIÓN

SIGME

FECHA DE EMISIÓN DEL INFORME	Día:	20	Mes:	06	Año:	2018

Proceso:	GESTIÓN TECNOLOGÍAS DE INFORMACIÓN
Subprocesos:	Desarrollo de Soluciones Informáticas, Sistema Único de Información y Gestión y Operación de la Infraestructura Tecnológica
Líder de Proceso / Jefe(s) Dependencia(s):	José Alfredo Ruiz Peralta
Objetivo de la Auditoría:	Evaluar el ambiente de control y administración del proceso Gestión Tecnologías de Información que atiende las necesidades de soluciones informáticas, de operación de la infraestructura tecnológica y del sistema único de información, en cumplimiento de las disposiciones establecidas y los requisitos legales relacionados en torno a la misión institucional, con enfoque en la administración de riesgos.
Alcance de la Auditoría:	La auditoría comprende la evaluación del estado de los controles internos de los subprocesos de la Gestión Tecnologías de Información (Desarrollo de Soluciones Informáticas, Sistema Único de Información y Gestión y Operación de la Infraestructura Tecnológica), de los mecanismos automáticos establecidos en el repositorio de información - SUI, de los proyectos de inversión y gasto TI y de los contratos de tecnología, con fecha de corte 31 de diciembre de 2017.

Jefe oficina de Control Interno	Auditor Líder
Myriam Herrera Durán	Luis Ernesto Vargas

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	16	Mes	03	Año	2018	Desde	16/03/2018 D / M / A	Hasta	15/06/2018 D / M / A	Día	20	Mes	06	Año	2018

1. METODOLOGÍA

- Se elaboró el plan de auditoría, el cual fue registrado en el aplicativo SIGME y se realizó comunicación de anuncio de la auditoria al Jefe de la Oficina de Informática, con radicado de memorando 20181400034793 del 16 de marzo de 2018.
- se realizó solicitud inicial de información, memorando 20181400040163, y efectuaron mesas de trabajo con los líderes de los subprocesos objeto de auditoria.
- Se aplicaron Normas de auditoría generalmente aceptadas (NAGAS), y las específicamente definidas en los criterios de documentos de referencia del plan de auditoria.
- Se realizó análisis de los documentos recibidos, se verificó las actividades que involucra la ejecución de los subprocesos y se revisó la información que se mantiene en las diferentes plataformas tecnológicas que los apoyan.

- Como resultado de la evaluación y pruebas de auditoría aplicadas, se proyectó el presente informe de auditoría a la Gestión Tecnologías de Información.
- La metodología aplicada y la documentación de las pruebas de auditoria y del proceso auditor, se conservan en la carpeta de papeles de trabajo de la Oficina de Control Interno.

2. DESARROLLO DEL INFORME

La Oficina de Control Interno de la Superintendencia de Servicios Públicos Domiciliarios, en cumplimiento de las funciones encomendadas por la Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado, en concordancia con la ejecución del Plan Anual de Auditorías Internas para la vigencia 2018 y con el fin de verificar la adecuada ejecución del sistema control interno y la eficiencia, eficacia y efectividad de los procesos, se realiza auditoría al proceso Gestión Tecnologías de Información.

2.1 GESTION TECNOLOGIAS DE INFORMACIÓN

Para el desarrollo de la auditoria, se tuvo como referente lo señalado en el artículo 8 del decreto 990 de 2002, en cuanto a las funciones de la Oficina de Informática, lo establecido en el decreto 415 de 2016, que motivo la reclasificación del proceso gestión tecnologías de información en estratégico y la caracterización del proceso definida para atender su propósito.

El proceso Gestión Tecnologías de Información tiene como fin gestionar el apropiado funcionamiento de la plataforma de Tecnología de Información y Comunicaciones, procesamiento y suministro de datos, seguridad informática y acorde a las buenas prácticas de seguridad de la información de acuerdo con las políticas de la entidad y las normas legales vigentes. Esta tarea la desarrolla con los subprocesos: Sistema Único de Información, Desarrollo de Soluciones Informáticas, y Gestión y Operación de la Infraestructura Tecnológica, Proceso y Riegos y Gestión de Proyectos de Inversión.

Para realizar esta labor se contó con la disposición de información y del equipo de la Oficina de Informática.

A continuación, se presentan el siguiente resultado del ejercicio auditor:

2.1.1. SISTEMA UNICO DE INFORMACION - SUI.

Este subproceso apoya la administración, mantenimiento y operación del Sistema Único de Información – SUI, a través de la atención de los requerimientos de información y soporte de acuerdo a la normatividad que para su efecto se expida o se encuentre vigente. *Inicia con el análisis y designación de responsables para atender las solicitudes y termina con la elaboración de planes de mejoramiento.*

En el desarrollo del cumplimiento del objetivo establecido, se incluyen los siguientes procedimientos:

- Gestión de trámites de habilitaciones, soporte y consultas internas de información (SUI-P-001), cuyo fin consiste en gestionar el trámite oportuno y con calidad de las solicitudes recibidas en el Grupo SUI, con el fin de solucionar los inconvenientes que se presentan en el cargue y consulta de información al SUI. Comienza con gestión de deshabilitaciones y habilitaciones, terminado con atención personalizada a prestadores de servicios.
- Diagnóstico y tratamiento de problemas en las herramientas de cargue SUI (SUI-P-002): identifica y analiza las causas de los problemas que se presentan en las herramientas de cargue y gestionar la solución de los mismos, para propender por la calidad y oportunidad de la información. Inicia con la detección del problema y termina con la comunicación de la solución implementada.

- Incorporación y redefinición de variables al SUI (SUI-P-003), apoya la implementación de nuevos requerimientos de información para los usuarios responsables de reportar la misma en el SUI. Inicia en el apoyo en la revisión de especificaciones y posterior prueba de las solicitudes de implementación de nuevos cargues de información al SUI.

- Publicación de Información SUI (SUI-P-004), gestiona la implementación de mecanismos que permitan la publicación de información en el SUI, para dar a conocer la Información del sector y así mismo facilitar la toma de decisiones en materia de servicios públicos domiciliarios.

El sistema SUI es una base de conocimiento de datos que recoge toda la información de las empresas prestadoras de servicios, prevista en la normatividad vigente para desarrollar la actividad de inspección, control y vigilancia, desde el año 2003 a la fecha.

Se ha realizado un acompañamiento de apoyo, en lo referente a la publicación de datos abiertos del sector de energía y gas combustible, para dar cumplimiento a los lineamientos establecidos en la ley de transparencia.

Se construye el catálogo de información de la base de datos SUI, la cual propende articular de forma automática y ordena: la norma, los formatos que involucra la norma, la descripción de los formatos y formularios del servicio público domiciliario, el diccionario de datos, los esquemas y tablas de la base de datos, el sitio de publicación de la norma, entre otros. Se avanza en el desarrollo de esta herramienta fundamental de la información SUI, para que esté alineada con toda la arquitectura de tecnología.

En concordancia con lo expuesto, y del resultado de la verificación realizada, se evidenció la siguiente situación:

Observación 1. Se permite visualizar las contraseñas privadas de los prestadores de servicios.

Se evidencia que las contraseñas (password) de las cuentas de usuario de los prestadores de servicios y en general de los usuarios que acceden por el sistema de autenticación SUA al Sistema Único de Información, se pueden visualizar por la consulta que se realiza a través de la herramienta de navegación del protocolo de acceso de directorios "JXplorer SUA". Este utilitario de consulta es utilizado por usuarios de informática y grupo SUI.

El numeral 3.13 política de alto nivel de seguridad de la información del "Código de Buen Gobierno" de noviembre de 2017, dominio A.9 Control de Acceso y Control de Acceso a Sistemas y Aplicaciones, determinan los lineamientos para la gestión de acceso de usuarios, y

el numeral 3.15 Política de privacidad, términos de uso y protección de datos personales del "Código de Buen Gobierno", señala: "*2. La entidad ha adoptado niveles de seguridad de protección de los datos personales, instalando medidas técnicas necesarias para evitar la pérdida, mal uso, alteración, accesos no autorizados y robo de los datos facilitados. La información personal proporcionada por el Usuario está asegurada por una clave de acceso que sólo él conoce. Por tanto, es el único responsable de mantener en secreto su clave...*"

Esta situación afecta la privacidad y el uso exclusivo de las claves de usuario, genera riesgos de manipulación y fuga de información.

Observación 2. Se habilitan usuarios del área de informática con acceso al sistema SUI, lo cual afecta privacidad de datos.

a. Se observa que existen usuarios del grupo de informática que tienen habilitado el acceso al Sistema Único de Información – SUI, a través de entrada a la plataforma del Sistema de Autenticación (SUA) y/o Base de Datos, lo cual genera riesgo de seguridad en la información por la función (gestión de software) técnica que este equipo de trabajo realiza, entre otros, los siguientes:

USUARIO BDD SUI	USUARIO LDAP-SUA	FUNCION	OBSERVACION
N/A	AFPRADA	INTERNAS	Por su función técnica no requiere acceso SUA.
N/A	ARAMIREZV	RETIRADA	Se encuentra activa en SUA el 04/05/2018. En listado del 21/06/2018 se reporta inactiva. Periodo Auditoria.
N/A	CIPRADA	INFRAESTRUCTURA	Por su función técnica no requiere acceso SUA.
JMARIN	JMARIN	INTERNAS	Por su función técnica no requiere acceso SUA.
N/A	JURDANETA	INFORMATICA PLANEACION	Por su función técnica no requiere acceso SUA.

N/A: No hay usuario

b. Se tiene una lista de 9 usuarios adscritos al grupo de "Informática", que ingresan por la plataforma de autenticación (SUA) al Sistema Único de Información – SUI, los cuales no tienen actividad directa relacionada con el sistema SUI.

c. Igualmente, se tiene una lista de 60 usuarios adscritos al rol "Grupo_SUI", con acceso de consulta a la base de datos, sin embargo, la oficina de coordinación, solamente reportó 28.

El numeral 3.13 política de alto nivel de seguridad de la información del "Código de Buen Gobierno" de noviembre de 2017, dominio A.9 Control de Acceso y Control de Acceso a Sistemas y Aplicaciones, determinan los lineamientos para la gestión de acceso de usuarios.

Por lo anterior, la institución se expone al riesgo de manipulación y fuga de información por permitir el ingreso a información no autorizada, de los prestadores de servicios, debido a la falta de administración de usuarios.

Observación 3. Se habilitan usuarios con ingreso a la base de datos, que, en algunos casos, ya cuentan con acceso normal al aplicativo, lo cual afecta disponibilidad del sistema y confidencialidad de la información.

De la revisión a la lista de usuarios de base de datos, se observó que no menos de 245 usuarios acceden a la base de datos SUI, de los cuales 22 de ellos también, tienen habilitado el ingreso normal al aplicativo, y están asociados, como grupo "DENER - Delegadas de Energía y Gas", así:

BDD SUI		LDAP-SUA		FUNCION	OBSERVACION
USUARIO	GRUPO	USUARIO	GRUPO		
JGUERRA	DEFAULT	JGUERRA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
JPLATA	DEFAULT	JPLATA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
JRENDON	PRO_ENERGIA	JRENDON	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
LTRIANA	GRUPO_SUI	LTRIANA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
MBELTRAN	PRO_ENERGIA	MBELTRAN	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
MPEREZ	GRUPO_SUI	MEPEREZ	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
OMURILLO	PRO-REPORTES	OMURILLO	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
ASEPULVEDA	GRUPO_SUI	ASEPULVEDA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
ASOSSA	DEFAULT	ASOSSA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
CCIBANEZ	PRO_CONTRIBUCION	CCIBANEZ	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
CRESTREPO	GUPO_SUI	CDRESTREPO	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
CEGUZMAN	PRO_REPORTES	CEGUZMAN	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
CVERA	GRUPO_SUI	CRVERA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
DAOSSA	PRO_ENERGIA	DAOSSA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
DBORDA	GRUPO_SUI	DBORDA	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
DMOZO	PRO_REPORTES	DMOZO	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
LCASTRO	GRUPO_SUI	GLCASTRO	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
GCISNEROS	PRO_ENERGIA	GPCISNER	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
GSAENZ	DEFAULT	GSAENZ	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
HANGEL	GRUPO_SUI	HANGEL	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
JCGIRALDO	DEFAULT	JCGIRALDO	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requeriría dos accesos a SUI
JCMARTINEZ	DEFAULT	JCMARTINEZ	DENER	DELEGADA DE ENERGIA Y GAS	Por su función no requiere acceso a SUI por BDD. No tiene consulta o reporte en detalle.

Se observa que para algunos usuarios el grupo al cual se encuentra adscrito en la base de datos no es concordante con el grupo al cual se encuentra adscrito en el sistema autenticador SUI.

El numeral 3.13 política de alto nivel de seguridad de la información del "Código de Buen Gobierno" de noviembre de 2017, dominio A.9 Control de Acceso y Control de Acceso a Sistemas y Aplicaciones y política para la construcción de sistemas seguros*: que indica: "La Oficina de Informática debe documentar y aplicar procedimientos de construcción de sistemas de información seguros basados en principios de construcción de seguridad y las debe incluir en el diseño de todas las capas de arquitectura"..*

Los ingresos a base de datos, por parte de usuarios de la operación, se debe, entre otras, a: la falta de revisión periódica a los accesos de los usuarios, las falencias que se tienen en la adecuada solución de

requerimientos, la falta de oportunidad en la solución, las deficiencias funcionales del aplicativo o la carencia de reportes y consultas de información.

Por consiguiente, se deteriora la disponibilidad del sistema, afecta criterios de seguridad y altera la estructura del sistema.

Observación 4. El sistema no tiene trazabilidad de los cambios de parámetros, en la cuenta de los usuarios de los prestadores de servicio, del SUI.

El ingreso a la operación de la plataforma del Sistema Único de Información, se realiza a través del sistema de autenticación - SUA, la cual facilita el acceso controlado de usuarios mediante el servicio de directorios (protocolo simplificado de acceso a directorios-LDAP), sin embargo, este servicio no tiene pistas de auditoria ni registro de las modificaciones que realizan los usuarios que tienen acceso a cambio de parámetros de las "cuentas de usuario" de las empresas prestadoras de servicio (cambios en: cuenta de usuario, contraseña, correo electrónico, teléfono, identificador, unidad organizativa, estado del usuario, tareas de usuario y tipo de usuario).

El artículo 2.2.9.1.2.1 del decreto 1078 de 2015, establece, los criterios para el componente TIC Gestión y el componente de seguridad y privacidad de la información. Numeral A.12.4 "Registro de eventos y generación de evidencias", de la declarativa de aplicabilidad de Seguridad de la Información ISO 27001:2013, sugerida por GEL.

Sin el registro automático de eventos que realizan los usuarios prestadores de servicio que acceden los parámetros de las cuentas, no se reconoce la intervención que hacen estos usuarios en el sistema, se afecta el seguimiento y control a los cambios de parámetro y se incumple la aceptación de la declarativa de seguridad de la información en el numeral A.12.4 registro de eventos y generación de evidencias.

Observación 5. El proceso de habilitación automática SUI presenta algunas inconsistencias, ya que se habilitan y/o retiran formatos y formularios que, en algunos casos, no corresponden al prestador de servicio.

Por lo menos un 40% (1.500 casos registrados en Aranda) de las solicitudes de habilitación y retiro son causadas por fallas en el proceso habilitador automático, en lo pertinente a la configuración de la matriz particular, la cual está asignando formatos y formularios que no son de cumplimiento del prestador de servicio y por lo cual se genera reclamación.

Código de Buen Gobierno, lineamientos para: "Control de acceso a sistemas y aplicaciones" y "Política para la construcción de sistemas seguros", señala: *"La Oficina de Informática debe documentar y aplicar procedimientos de construcción de sistemas de información seguros basados en principios de construcción de seguridad y las debe incluir en el diseño de todas las capas de arquitectura".*

Esta situación ocasiona importante demanda de este servicio, afecta credibilidad del sistema y genera carga operativa.

Observación 6. Se realiza de forma manual trámites de habilitaciones, retiros y reversiones de formatos y formularios de los prestadores de servicio en la base de datos SUI, lo cual posibilita fallas en la operación y deteriora seguridad de datos.

Si bien se cumplen las actividades y autorizaciones que señala el procedimiento de gestión de trámites de habilitaciones, deshabilitaciones y reversiones (SUI-P-001), se observa que la solución a las solicitudes de estos trámites, se realiza de forma manual en la plataforma SUI. Los analistas de desarrollo de software del grupo SUI ejecutan comandos con la herramienta (SQL), los cuales permiten ingresar a la base de datos, con el fin de impactar los archivos y datos (tablas) en la forma que han sido requeridos, sin contar con trazabilidad automática en la base de datos.

Código de Buen Gobierno, lineamientos para: "Control de acceso a sistemas y aplicaciones" y "Política para la construcción de sistemas seguros", señala: *"La Oficina de Informática debe documentar y aplicar procedimientos de construcción de sistemas de información seguros basados en principios de construcción de seguridad y las debe incluir en el diseño de todas las capas de arquitectura".*

Esta es una práctica insegura porque facilita el error y no tiene trazabilidad automática del trámite realizado en la base de datos.

Observación 7. No hay instructivos que detallen las características técnicas de las validaciones internas y externas de los formatos de cargue masivo, anexos a los actos administrativos.

La normatividad que se expide sobre el sistema único de información de servicios públicos domiciliarios, determina y especifica la estructura de la información que tendrán los archivos que la conforman. El cargue masivo de esta información que realiza el prestador del Servicio, lo realiza a través de los archivos que han sido validados externa e internamente y cumplen con la estructura de información definida en la norma (anexo). Sin embargo, no se cuenta con instructivo público, que detalle las características de la información (longitud de los campos, descripción y característica del campo) y de las validaciones del servicio al cual pertenece el formato que va a cargar el prestador de servicio.

El artículo 2.2.9.1.2.1 del decreto 1078 de 2015, establece, los criterios para el componente TIC Gestión, en lo referente a la documentación de los sistemas de información y determina lineamientos (LI.SIS.16 Manual del usuario, técnico y de operación de los sistemas de información), de Gobierno en Línea, para su desarrollo.

Independientemente, a la capacitación de instrucción manejo del sistema, dirigida al prestador del servicio, se generan solicitudes para apoyar el cargue de información masiva en archivo, generando reprocesos por la falta de ayudas en la publicación de estructura de datos y archivos de cargue.

2.1.2. DESARROLLO DE SOLUCIONES INFORMATICAS.

Este subproceso (SI-SP-001) tiene como objetivo crear nuevas soluciones informáticas, actualizar o mejorar las existentes, siguiendo los procedimientos de desarrollo y mantenimiento definidos por la Oficina de Informática, con el fin de suplir las necesidades de los procesos de la Superservicios en el cumplimiento de su misión.

Se establecen los siguientes procedimientos, para la consecución del propósito indicado:

- Desarrollo de la solución informática (SI-P-001): la cual consiste en desarrollar soluciones informáticas de acuerdo a los requerimientos especificados por los proveedores del proceso y a los lineamientos, procedimientos, instructivos, formatos, estándares de la Oficina de Informática que se encuentran definidos en el Sistema de Gestión de Calidad, con el fin de apoyar el cumplimiento de la misión de la Superintendencia de Servicios Públicos Domiciliarios
- Seguimiento y validación de la solución adquirida (SI-P-002), implica realizar seguimiento y validación con el usuario y el proveedor a la solución informática adquirida, a partir de la revisión del cumplimiento de los requerimientos establecidos, con el fin de contar con una solución informática que apoye el cumplimiento de la misión de la Superintendencia de Servicios Públicos Domiciliarios.
- Mantenimiento de la solución informática (SI-P-003), realiza mantenimientos y mejoramientos a las soluciones informáticas existentes, a través de actividades de requerimientos, desarrollo, pruebas y puesta en producción, para atender las necesidades de la Entidad relacionadas con ajustes a las aplicaciones, para que brinden mejor apoyo, control, oportunidad y veracidad en las labores que se realizan de apoyo al cumplimiento de la misión.

Para atender el desarrollo de soluciones informáticas, la oficina está organizada en equipos de trabajo, que atiende requerimientos informáticos referentes al sistema único de información- SUI, cubren soluciones para el sistema de gestión documental ORFEO y abordan necesidades de los restantes sistemas internos. Además, cuenta con un equipo de trabajo especializado en realizar ejercicios de pruebas sobre los cambios efectuados al software, los cuales son validados funcionalmente para su ingreso al ambiente productivo.

El equipo de desarrollo que apoya la plataforma SUI, es un equipo especializado en realizar las tareas de implementación técnica de las solicitudes realizadas por las áreas misionales, en cuanto al SUI.

Es importante, mencionar el sistema Orfeo, en cuanto a que apoya todo el sistema de gestión documental, teniendo en cuenta criterios definidos por el Archivo General de la Nación.

De acuerdo con lo anteriormente indicado y como resultado de la verificación realizada por el equipo auditor, se evidenció la siguiente situación:

Observación 8. Se evidencia que no hay resultados del ejercicio de las pruebas "no funcionales" al software modificado o elaborado, lo cual podría afectar operatividad y seguridad del sistema.

Se diligencia el formato SI-F-007 como documento requisito para planear los requerimientos no funcionales (seguridad, rendimiento, disponibilidad, capacidad, fiabilidad, portabilidad, mantenibilidad; escalabilidad, reusabilidad, interfaces, usabilidad) que debe cumplir el software que ha sido elaborado o modificado, para permitir su ingreso al ambiente productivo; sin embargo, se evidencia la falta y necesidad de resultados de este tipo de pruebas, al software que ingresa a producción.

Actualmente, el formato SI-F-007 es opcional, lo cual afecta el desempeño de las pruebas de software.

Expediente 20171600208000 8E

Radicado	Anexo	Descripción	Observación
20171600067843	Anexo 11	Toneladas Aprovechables Mod..Administrador	No hay resultado de pruebas no funcionales
	anexo 14	Formato SI-F-007 – Cargue Aprovechamiento	No hay resultado de pruebas no funcionales
20171600062403	anexo 19	Formato SI-F-007 - Administración de Localidades – ZNI	No hay resultado de pruebas no funcionales
20171600050313	anexo 9 y 12	Formato S-F-007 –Verificación Tarifaria de Aseo	No hay resultado de pruebas no funcionales

El artículo 2.2.9.1.2.1 del decreto 1078 de 2015, establece, los criterios para el componente TIC Gestión y el componente de seguridad y privacidad de la información. Lineamientos LI.SIS.14 Plan de pruebas durante el ciclo de vida de los sistemas de información de Gobierno en Línea. Declarativa de aplicabilidad A.14.2.8 Pruebas de seguridad de sistemas ISO 27001:2013, sugerida por GEL.

La actividad 4. "Gestionar pruebas de la solución informática del Procedimiento Desarrollo de la Solución Informática (SI-SP-001), señala tareas para la gestión de pruebas.

Lo anterior expone a inadecuada funcionalidad de los sistemas y afecta seguridad de la información.

Observación 9. Se realizan pruebas de software en el ambiente productivo, lo cual genera riesgos de confiabilidad y disponibilidad de la información.

La actividad 10 del "Procedimiento Mantenimiento de la Solución Informática (SI-P-003)" determina que: "*La verificación del despliegue de la solución informática se realiza mediante las pruebas en el ambiente de producción las cuales se programan con la solicitud de cambio…*"; sin embargo, esta disposición es contraria a la declaración de aplicabilidad SGSI-F-001, en cuanto a la separación de ambientes para reducir riesgos de acceso o cambios, así mismo, al Código de Buen Gobierno, en referente al control de acceso a sistemas y aplicaciones y las mejores prácticas de seguridad de la información, adoptadas por los lineamientos GEL.

Además, se observa que usuarios de sistemas designados para el ejercicio de pruebas de software en la plataforma de pruebas, también realizan validaciones en el ambiente productivo.

El numeral 3.13 política para la construcción de sistemas seguros del "Código de Buen Gobierno" de noviembre de 2017, define lineamientos, en:

- El dominio: "A.14 Adquisición, desarrollo y mantenimiento de Sistemas", en cuanto a: aplicar los principios de construcción de sistema seguros a todos los nuevos desarrollos o cambios en los paquetes de software para garantizar la seguridad de la información).
- y el dominio: "A.9 Control de Acceso y Control de Acceso a Sistemas y Aplicaciones", en lo referente a los lineamientos para garantizar la seguridad en ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción)

Control A.12.1.4 separación de los ambientes de desarrollo, pruebas y operaciones, para reducir los riesgos de acceso a cambios no autorizados al ambiente de operación, definido en la declarativa de aplicabilidad del estándar de seguridad ISO 27001, la cual es sugerida por Gobierno en Línea.

Esta situación afecta la seguridad de la información, independientemente de los recursos que se utilicen en el ambiente de producción para realizar las pruebas, ya que el software ha sido probado y autorizado para su productividad.

Observación 10. Se observan deficiencias en los procedimientos de desarrollo de soluciones informáticas en cuanto al alcance de la solución en el sistema, el tiempo requerido, la disponibilidad de los recursos técnicos, el impacto funcional en el sistema y la calidad del software, como componentes metodológicos.

Los procedimientos, instructivos y manuales describen las directrices y actividades (análisis de la solicitud, definición de requerimientos, diseño de la solución, desarrollo, gestión de pruebas, uso y apropiación y documentación) que se realizan para el desarrollo, mantenimiento o adquisición de soluciones informáticas; Sin embargo, las tareas que se realizan no son suficientes para determinar el alcance de la solución, el tiempo de desarrollo del proyecto, la disponibilidad de los recursos técnicos (software y hardware) y la calidad del software, las cuales son importantes precisar dentro de un desarrollo metodológico de software y en un ciclo de vida del sistema, previamente definidos. con el fin de entregar resultados de software con funcionalidades de solución integral que atienda las necesidades del usuario.

Además, estas actividades definidas para el desarrollo y solución de software no se integran con arquitecturas de solución de sistemas de información, arquitectura de información, estrategias de uso y apropiación y en general con la arquitectura TI, en proceso de implementación.

El subproceso Desarrollo de la Solución Informática (SI-P-001) no establece los criterios de análisis que se tendrían en cuenta para clasificar las soluciones informáticas en nuevo desarrollo, solución adquirida o solución de mantenimiento, los cuales dependen del alcance del trabajo y necesidades del servicio.

El artículo 2.2.9.1.2.1 del decreto 1078 de 2015, establece, los criterios para el componente TIC Gestión, los lineamientos LI.SIS.03 Arquitecturas de referencia de sistemas de información, LI.SIS.04 Arquitecturas de solución de sistemas de información, LI.SIS.05 Metodología de referencia para el desarrollo de sistemas de información, LI-SIS-18 Estrategia de mantenimiento de los sistemas de información, de Gobierno en Línea, los cuales son importante desarrollar

Esta situación, genera riesgos en la oportunidad de entrega de software, funcionalidad y calidad del sistema.

2.1.3. GESTION Y OPERACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA.

El objetivo gestionar y operar la infraestructura tecnológica, asegurando la disponibilidad de los servicios de tecnología de información (TI) que administra la Oficina de Informática, para el cumplimiento de la misión de la entidad.

En cumplimiento del objetivo establecido, se identifican los siguientes procedimientos:

- Gestión de incidentes (GT-P-001), restaura la operación normal de los servicios de TI (Tecnología de la Información) para dar continuidad al servicio y con mínimo impacto a la Entidad. Inicia con el registro del incidente en la herramienta de gestión de servicios de TI y finaliza con el cierre.

- Gestión de problemas (GT-P-002): analizar y solucionar los incidentes mayores y problemas sobre los servicios de TI (Tecnología de la Información), para garantizar la continuidad de los servicios minimizando el impacto a los usuarios/clientes.

- Gestión de solicitudes de servicio (GT-P-003), recibe, evalúa y ejecuta de forma ordenada y controlada los requerimientos de los usuarios sobre los servicios de TI prestados por la Oficina de Informática.

- Gestión de cambios (GT-P-004), recibe y analiza los cambios solicitados para que sean valorados, aprobados e implementados de manera planeada y controlada, para reducir los riesgos a los usuarios/clientes de los servicios de TI (Tecnología de Información) y minimizar el impacto de los mismos.

- Gestión de versiones (GT-P-005), verifica y/o asigna la versión al Ítem de Configuración (CI) involucrado en el cambio, de acuerdo al manual de versionamiento adoptado por la Oficina de Informática, con el fin de contar con un adecuado control de las versiones de los CI del software, hardware y documentación que soportan la operación de la plataforma tecnológica de la Entidad.

- Gestión de la configuración (GT-P-006), Identifica, registra, controla y verifica todos los elementos o items de configuración (CIs) del repositorio de gestión de la configuración, para mantener actualizada la información y las interrelaciones de la infraestructura tecnológica.

- Copias de respaldo de servidores, gestiona las copias de respaldo y verifica la ejecución de la programación en la herramienta de backup.

- Mantenimientos programados sobre la infraestructura TI, realiza mantenimiento preventivo programado sobre la infraestructura de TI acorde a la programación.

- Informes de capacidad y obsolescencia, monitorea la disponibilidad de los servicios TI ofrecidos y la capacidad de TI disponible de la infraestructura, junto con el nivel de obsolescencia, a fin de genera los informes y alertas.

Se observa que se hizo una adecuación física al centro de datos, en la sede de la Cll 84, la cual le permite tener un mejor control periférico y del centro de control de la red, asi como de la distribución y organización interna de los equipos de procesamiento y comunicaciones.

Para la atención de la gestión y operación la infraestructura tecnológica, la Oficina de Informática, cuenta, entre otros, con el proveedor "INFOTIC", que presta los servicios de tecnologías de información y comunicaciones, así como los demás bienes y servicios requeridos para la operación y mejora continua de los servicios TIC de la Superservicios, incluida la gestión y administración, bajo la modalidad de outsourcing informático.

Esta labor se enmarca en seis servicios principales, las cuales son:

- Centro de procesamiento de datos (CPD): efectuar la gestión de la infraestructura tecnológica alojada en los centros de datos.

- Networking (Net): mantener la conectividad de la red de datos, telefonía y video, en toda su infraestructura.
- Mesa de servicios (MDS): determinar un punto de contacto para la atención de necesidades y requerimientos de todos los asuntos relacionados con los servicios de tecnologías de información y comunicaciones.
- Seguridad: prestar la gestión, administración, operación, integración e interoperabilidad de servicios de tecnologías de información y comunicaciones en términos de seguridad informática y seguridad de la información.
- Gestión Global (GLO): realizar la gestión, integración, interoperabilidad, administración, control, seguimiento y monitoreo de los servicios del outsourcing.
- Equipo de trabajo: suministrar el recurso humano idóneo y suficiente para operar el servicio.

En atención a lo arriba expresado y teniendo en cuenta el resultado de la revisión efectuada, se observó:

Observación 11. Se observan debilidades en los mecanismos de despliegue de software, en el ambiente de producción.

El ingreso de software al ambiente de producción, se realiza de dos formas. Una por despliegue de software de aplicación, la cual consiste en copiar el código fuente en la ruta indicada por el usuario de informática y otra por despliegue de base de datos, que comprende la copia del software (script) en los esquemas de la base de datos de producción. En ambos procesos no hay bitácora automática de la copia, compilación (conversión del software a objeto) y versión de la configuración del software transportado en ambiente productivo.

Además, en el sistema Aranda y Orfeo, en lo referente a los casos de soluciones de software, se encuentra adjunta a la documentación descriptiva del caso (requerimiento o cambio), el código fuente del software sin la debida protección, el cual el grupo de desarrollo de soluciones informáticas ha construido.

De la revisión a los requerimientos y cambios del sistema Aranda, se observó el registro de 7.600 casos referentes a fallas en software del sistema SUI, sistema Orfeo y otros aplicativos internos, para la vigencia 2017, de los cuales 76 solicitudes implicaron transporte de software al ambiente de producción (controles de cambio), y solamente 42 se identificaron como servicio "software desplegado al ambiente de producción", en Aranda. Esta situación muestra la parcialidad y manualidad del control que se tiene sobre el servicio.

El numeral 3.13 política de alto nivel de seguridad de la información del "Código de Buen Gobierno" de noviembre de 2017, en cuanto a los lineamientos de Control de Acceso a Sistemas y Aplicaciones, establece en lo referente a "*6. El líder de seguridad de la información, debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información*".
Actividad 3, procedimiento gestión de versiones (GT-P-005), en cuanto a verificar y asignar la versión para cambio de versión.

Lo expuesto, afecta la debida seguridad que se debe preservar en el código fuente y objeto del sistema, y en general, la información.

Observación 12. No es adecuada la gestión de aprobación de cambios.

El equipo de aprobación de cambios, lo conforma el gestor de cambios del Outsourcing (responsable del comité gestión de cambios), el gestor representante de infraestructura SSPD y el usuario solicitante del cambio. El gestor de cambios convocó a 49 sesiones al equipo de aprobación de cambios, durante la vigencia de 2017. El equipo sesionó en algunos casos de forma virtual (telefónica) y en otros presencial.

Las actividades que realiza el equipo de aprobación de cambios se circunscribe a validar los cambios normales y de emergencia, previamente ejecutados. El cambio estándar normalmente ingresa al ambiente productivo, dado que cuenta con una garantía de pre-aprobado, de acuerdo con una lista definida.

No obstante, se observa que las funciones de gestión del equipo de aprobación de cambios y las del gestor de cambios, se encuentran agrupadas en el técnico especializado del Outsourcing. Además, independientemente, a las funciones que realiza el gestor representante de infraestructura de la Oficina de Informática en el equipo de aprobación, se evidencia que no se efectúan tareas de supervisión, seguimiento al alcance, impacto funcional, impacto no funcional (de seguridad) del cambio de la gestión de la infraestructura, del software y de la gestión de operación y funcionalidad de los sistemas, análisis de tendencias de cambios, alternativas de mejora.

El procedimiento gestión de cambios (GT-P-004) establece las actividades que se realizan para recibir y analizar los cambios solicitados para que sean valorados, aprobados e implementados de manera planeada y controlada.

El artículo 2.2.9.1.2.1 del decreto 1078 de 2015, establece, los criterios para el componente TIC Gestión y el componente de seguridad y privacidad de la información. Lineamientos LI.SIS.17 "Gestión (actualización y requerimientos) de cambio de los sistemas de información". Declarativa de aplicabilidad A.12.1.2 Gestión de cambios ISO 27001:2013, sugerida por GEL.

Se afecta seguridad de la información, por el alcance especifico que tiene el control de cambios de software y hardware, la cual impactará la infraestructura, los sistemas de procesamiento y en general la operación.

Observación 13. Se tienen debilidades en el registro de la versión de software que ingresa a producción.

El numeral 3.13 control de acceso a sistemas y aplicaciones del Código de buen gobierno, asigna unas funciones para el "Administrador de Programas Fuentes", quien tendrá entre otras, la custodia de los programas fuentes, sin embargo, se observó que esta función no se realiza.

De otra parte, la actividad 8 referente a la Gestión de Versiones de Software y Hardware del procedimiento Gestión y Operación de la Infraestructura Tecnológica (GT-SP-001), relaciona las actividades que debe realizar el gestor de versiones; sin embargo, esta función no se encuentra centralizada en un gestor de proceso de versiones, sino que está dispersa en cada uno de los grupos desarrolladores de software que llevan un control en el ambiente de pruebas y desarrollo y no en la producción, la cual deteriora el registro de versión del software productivo.

No se encuentra activa en el ambiente de producción la herramienta registro de versiones de software - Subversión SVB-, que es un control organizado y expedito del software, la cual opera en los ambientes de desarrollo y pruebas, sin ser vital el control. Esta herramienta la utiliza el grupo de analistas y desarrolladores de software, para la organización del código fuente y objeto que se encuentra en construcción.

En observancia del El numeral 3.13 política de alto nivel de seguridad de la información del "Código de Buen Gobierno" de noviembre de 2017, en cuanto a los lineamientos de Control de Acceso a Sistemas y Aplicaciones, en lo referente a "*6. El líder de seguridad de la información, debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información*". Actividad 3, procedimiento gestión de versiones (GT-P-005), en cuanto a verificar y asignar la versión para cambio de versión.

De lo comentado, no se sigue los procedimientos establecidos para el versionamiento, no es adecuada la catalogación y el control del software es deficiente, desconociendo su estado en producción. Esta situación afecta el control y confidencialidad del software.

Observación 14. Se evidencian debilidades de seguimiento y control a los servicios de mesa de ayuda.

Se realizó una revisión de 11 casos (requerimientos e incidentes) reportados a la mesa de ayuda (del sistema Aranda), de los cuales se encontró que 9 presentan la siguiente situación:

Nro. Caso Aranda	Fecha	Observación
95878	16/09/2017	Se solicita mantenimiento preventivo del equipo con serial número MXJ84303N7. Se realizó tratamiento de software. Mal categorizado.
95888	16/09/2017	Se solicita mantenimiento preventivo del equipo con serial número MXJ84303PX. Se realizó tratamiento de software. Mal categorizado.
89039	15/06/2017	Se categoriza mantenimiento preventivo. Se solicita verificar el escáner, en el momento de realizar escaneos queda una línea negra vertical en el documento digitalizado. Se verifica unas ip en la red con alerta de virus y se procede a realizar limpieza de los lectores ópticos del escáner. Mal categorizado.
82106	08/03/2017	Se solicita mantenimiento preventivo al equipo con placa # 17701. Se anexa ficha técnica mantenimiento preventivo firmada por el usuario, en donde se indica la verificación funcionamiento inicial y encendido del equipo. Falta incluir trazabilidad de actividades que implica el mantenimiento preventivo.
82048	17/03/2017	Se solicita mantenimiento preventivo al equipo con placa # 17722. Se anexa ficha técnica mantenimiento preventivo firmada por el usuario. Se indica la verificación funcionamiento inicial y encendido del equipo. Falta incluir trazabilidad de actividades que implica mantenimiento preventivo.
82041	07/03/2017	Se solicita mantenimiento preventivo al equipo con placa # 11855. Se anexa ficha técnica mantenimiento preventivo firmada por el usuario. No hay trazabilidad de actividades realizadas en el mantenimiento preventivo.
80714	15/02/2017	Se solicita mantenimiento correctivo del equipo con placa 14997. Se realizó tratamiento de software. Mal categorizado.
88927	14/06/2017	Se solicita mantenimiento preventivo al equipo MXL242. No hay ficha técnica mantenimiento preventivo firmada por el usuario.
100918, 103613, 107410 109751,	06/12/2017 27/12/2017 31/01/2018 21/02/2018	Se solicita acceso de lectura y copiado en la carpeta OCI. Cierre:22/12/2017 Se solicita descargar radicado de la bandeja de tareas y proceso. Cierre: 02/02/2018 Se solicitó creación de usuario. cierre: 05/02/2018 Se solicitaron revisión accesos de la carpeta OCI. Cierre 27/02/2018 No hay oportunidad en la atención de la solicitud.

De lo anterior, se observa insuficiente seguimiento a solución de casos de la mesa de ayuda registrados en Aranda, en cuanto a oportunidad, adecuada entrega y clasificación del servicio, por parte de las coordinaciones de gestión.

El artículo 2.2.9.1.2.1 del decreto 1078 de 2015, establece, los criterios para el componente TIC Gestión y el componente de seguridad y privacidad de la información. Lineamientos LI.ST.09 "Mesa de servicio". Procedimientos para la gestión de incidentes (GT-P-001), problemas (GT-P-002), solicitudes de servicio (GT-P-003), cambios (GT-P-004).

El numeral 3.13 política de alto nivel de seguridad de la información del "Código de Buen Gobierno" de noviembre de 2017, en cuanto al dominio A.16 - Gestión de incidentes de seguridad de la información.

Se afecta la atención de solicitudes de servicio, por deficiencias en la administración de los casos de mesa de ayuda.

2.1.3.1 CONTRATISTA INFOTIC

Observación 15. De la revisión realizada al contrato 819 de 2017, contratista INFOTIC, la cual se formalizó el 25 de octubre de 2017, con plazo de ejecución de 8 meses, se encontró las actividades específicas del servicio de Seguridad (numeral 3 del contrato), en el siguiente estado:

ACTIVIDADES	OBSERVACIÓN
1.Elaborar plan estratégico de seguridad, la cual debe cumplir con las políticas del SGSI de la Superservicios.	El proveedor suministró un plan de gestión de la seguridad informática.
2.Elaborar y actualizar las políticas de seguridad necesarias para la gestión y administración de las tecnologías de seguridad que prestan servicio a la Superservicios. Estas políticas son validadas por la Superservicios.	Se encuentra pendiente de publicar.
5.Elaborar y mantener actualizado de acuerdo a los cambios presentados en la presentación de los servicios un plan de contingencia dentro el alcance del contrato. Este plan será validado por la Superservicios.	De la revisión al documento "Plan de Contingencia versión 1.5, febrero de 2018", suministrado por la Oficina de Informática, como respuesta a la obligación establecida con el proveedor INFOTIC, en lo referente a plan de contingencia, plan de recuperación de desastres y ejecución de pruebas, se observó que este documento corresponde a una relación de disponibilidad de servicios informáticos, incompleto. El documento referencia procedimientos de proveedores que no tienen relación vigente con la SSPD, algunos manuales se encuentran desactualizados (por ejemplo la configuración de servicios de red), el informe no incluye todas las plataformas tecnológicas (solamente linux); no es completo el contenido, en lo pertinente a los criterios que es conveniente considerar en un plan de recuperación de desastre y plan de contingencia (por ejemplo: análisis del impacto de negocio, BIA, valoración de riesgos y controles, estrategias de recuperación, procedimientos detallados para la restauración de un sistema, pruebas, entrenamiento y ejercicios, y mantenimiento, entre otros).
6. Cuando sea requerido por la Superservicios ejecutar pruebas del plan de contingencia dentro del alcance del contrato.	
7. Cuando sea requerido por necesidades del servicio ejecutar las actividades del plan de contingencia dentro del alcance del contrato.	
8.Elaborar una propuesta de un plan de recuperación de desastres (DRP) para los servicios, TIC dentro del alcance del contrato, avalados por la Superservicios.	
11.Efectuar el tercer mes después del inicio del contrato y semestralmente durante la operación, la de detección y análisis de vulnerabilidades ejecutado por un profesional Ethical Hacking Certified por el EC-Council. Elaborar un plan de remediación frente a las vulnerabilidades detectadas.	Se han implementado acciones correctivas parcialmente.
Matriz de riesgos gestionados de seguridad de la información.	Pendiente de ejecutar. Los riesgos de seguridad de la información, los cuales deben integrarse a los riesgos del proceso y de la entidad, en concordancia con las directrices establecidas por el DAFP.

Numeral 5.13 política de alto nivel de seguridad de la información, (Política para la continuidad de seguridad de la información Dominio A.17) del Código de Ética y Buen Gobierno, la cual determina los lineamientos a seguir para el plan e continuidad y la planificación de la continuidad de la seguridad de la información.
Numeral 8.4 "Plan de Contingencia" del Manual de Seguridad Informática (TI-M-001), la cual señala que se debe realizar por lo menos una prueba aleatoria al año a algunos de los escenarios del plan de contingencia por parte de la oficina informática, con el fin de verificar la efectividad.

De lo anterior, se debilita el resultado de las actividades que tienen lento avance.

2.1.4. PROCESO Y RIESGOS

Durante la ejecución de la auditoria y teniendo en cuenta el periodo de revisión, se observó que el proceso Gestión de Tecnologías de la Información, cuenta con la siguiente documentación: Subproceso Gestión y operación de Infraestructura Tecnológica, que incluye 6 procedimientos, 3 manuales, 3 instructivos y 6 formatos; Subproceso Desarrollo de Soluciones Informáticas que incluye 3 procedimientos, 1 manual, 3 instructivos y 16 formatos; Subproceso Sistema Único de Información SIU que incluye 4 procedimientos, 1 instructivo, 6 manuales y 4 formatos y cuenta con siete (7) riesgos definidos en su mapa.

Observación 16. En la revisión de la documentación arriba citada, se identificó que en algunos casos se duplica las actividades que se desarrollan al interior del proceso y en otros casos no incluye validaciones y/o actividades que actualmente se realizan.

Realizar una revisión del proceso, identificando la estructura y elementos que intervienen en él, identificando las actividades, controles, riesgos, flujos de información, soportes tecnológicos, apoyos administrativos, recursos, entre otros.

Es necesario comentar que la oficina de tecnologías de la información, actualmente se encuentra desarrollando el ejercicio de rediseño de procesos.

Observación 17. No se identifica en la Matriz de Riesgos del Proceso, que se encuentren definidos de manera adecuada los controles que deben aplicarse para abordar la prevención y mitigación de los riesgos; esta situación demuestra desconocimiento por parte de los líderes de proceso y sus equipos de trabajo, sobre la conceptualización y aplicación de la Metodología para la Administración del Riesgo definida por el departamento Administrativo de la Función Pública – DAFP.

Es importante atender las observaciones, conclusiones y recomendaciones emitidas en el Informe 20171400012170 3 del 14 de diciembre de 2017 sobre la auditoria de gestión al Proceso de Mejora Continua – Procedimiento Gestión del Riesgo. (Consultar Acta de Asesoría en Riesgos).

Se recomienda que la Oficina Asesora de Planeación en articulación con los líderes de proceso, implemente ejercicios de asesoría, facilitación metodológica, documentación y aplicación de controles sobre las oportunidades de mejora identificadas en los ejercicios de auditoria.

Esta observación se trasladará a Oficina asesora de planeación.

2.1.5. PROYECTOS DE INVERSION

La Oficina de tecnologías de la Información, tiene a cargo el Proyecto de Inversión No.152 denominado "Fortalecimiento de los Sistemas de Información en la Superintendencia de Servicios Públicos Domiciliarios", el cual tiene por objeto, "Contar con la plataforma tecnológica adecuada para cumplir las funciones asignadas a la Superintendencia de Servicios Públicos Domiciliarios.

Este ejercicio de auditoria se permite precisar, que la revisión adelantada en torno a l Proyecto de Inversión de la Oficina de Tecnologías de la Información, considera tres aspectos relevantes:

1. Estado acumulado del proyecto en torno al cumplimiento de productos
2. Ejecución del proyecto durante la vigencia 2017, los soportes de avance y la ejecución presupuestal
3. Metodología de seguimiento de proyecto adelantada al Interior de la Oficina TIC.

2.1.5.1. Estado del Proyecto en el Tiempo

El Horizonte del proyecto abarca desde la vigencia 2013 hasta la vigencia 2018; los recursos asignados para el desarrollo del proyecto durante los cinco (5) años de duración, corresponden a ($45.687.599.988,00) de los cuales se identifica una ejecución acumulada al 31 de mayo de 2018, equivalente al 84,67%, tal como se identifica a continuación:

VIGENCIAS	SOLICITADO PROYECTO	INICIAL	VIGENTE	Presupuesto Comprometido (Registros)	Presupuesto Obligado	Saldo por comprometer	% Ejecución	Pagos Dic 31 x Vigencia	% Pagos
2013	$ 8.497.000.000,00	$ 6.407.939.988,00	$ 6.407.939.988,00	$ 5.790.129.658,00	$ 4.851.171.206,00	$ 938.958.452,00	90,36%	$ 3.301.994.688,00	57,03%
2014	$ 7.251.886.540,00	$ 6.520.000.000,00	$ 6.520.000.000,00	$ 6.386.341.081,33	$ 6.168.848.755,33	$ 351.151.244,67	97,95%	$ 5.010.420.047,33	78,46%
2015	$ 8.525.000.000,00	$ 9.025.000.000,00	$ 7.630.660.000,00	$ 7.511.219.449,83	$ 7.338.345.880,99	$ 292.314.119,01	98,43%	$ 3.675.425.212,00	48,93%
2016	$ 9.165.000.000,00	$ 9.300.000.000,00	$ 8.109.000.000,00	$ 7.366.763.659,77	$ 6.193.575.091,78	$ 1.915.424.908,22	90,85%	$ 3.690.662.447,52	50,10%
2017	$ 9.500.000.000,00	$ 8.200.000.000,00	$ 8.020.000.000,00	$ 7.648.559.366,49	$ 7.039.452.803,88	$ 980.547.196,12	95,37%	$ 5.187.852.381,09	67,83%
2018	$ 9.650.000.000,00	$ 9.000.000.000,00	$ 9.000.000.000,00	$ 3.980.589.593,49	$ 1.434.667.277,00	$ 7.605.032.723,00	44,23%	$ 1.488.652.897,00	37,40%
TOTALES	**$ 52.588.886.540,00**	**$ 48.452.939.988,00**	**$ 45.687.599.988,00**	**$ 38.683.602.808,91**	**$ 33.026.061.014,98**	**$ 12.083.428.643,02**	**84,67%**	**$ 22.355.007.672,94**	**57,79%**

El proyecto consta de cuatro objetivos específicos con un total de catorce (14) Productos y dieciséis (17) Indicadores de Producto; a partir de la información reportada en el Sistema de Seguimiento de Proyectos de Inversión SPI, se identifica, que con corte a mayo 31 de 2018 se tiene un avance de Productos en promedio del 92%, es decir un total de nueve (9) indicadores de producto terminado y ocho (8) indicadores de producto que aún se encuentran en ejecución, que no han llegado al 100% en su desarrollo.

2.1.5.2. *Ejecución del Proyecto de Inversión Vigencia 2017*

Objetivos Proyecto	Producto	Actividades	Presupuesto Inicial	Presupuesto Vigente	% Variación	Presupuesto Comprometido (Registros)	Saldo por comprometer	% Eje	Pagos Dic 31/2017	% Pag
Implementar y mantener actualizado un sistema de seguridad de la información, que proteja las redes de la entidad de riesgos informáticos.	Plataforma tecnológica de seguridad de la información	Implementar las acciones de mejora resultado del análisis de seguridad de la Información	$ 30.000.000,00	$ 30.000.000,00	0%	$ 29.150.240,00	$ 849.760,00	97%	$ 29.150.240,00	0,4%
		OBJETIVO 1	$ 30.000.000,00	$ 30.000.000,00	0%	$ 29.150.240,00	$ 849.760,00	97%	$ 29.150.240,00	0,4%
Desarrollar y mejorar los sistemas de información y aplicativos que soporten la adecuada prestación de los servicios a cargo de la entidad.	Sistemas de Información	Implementar las solicitudes de actualización a los sistemas de información para atender los requerimientos de las diferentes áreas de la Superservicios.	$ 450.000.000,00	$ 420.000.000,00	-7%	$ 336.298.335,00	$ 83.701.665,00	80%	$ 330.465.001,00	4,1%
	Aplicaciones y/o Módulos nuevos desarrollados o implementados	Analizar y/o desarrollar y/o implementar los sistemas de información de la SSPD (SUI y Aplicaciones internas)	$ 1.523.732.500,00	$ 1.453.732.500,00	-5%	$ 1.428.582.892,33	$ 25.149.607,67	98%	$ 1.403.622.892,33	17,5%
		Fortalecer el Sistema de Información Geográfico para la Superservicios	$ 200.000.000,00	$ 200.000.000,00	0%	$ 188.156.776,66	$ 11.843.223,34	94%	$ 188.156.776,66	2,3%
		Actualizar el sistema Business Process Management - BPM de la SUPERSERVICIOS	$ 626.267.500,00	$ 626.267.500,00	0%	$ 199.999.999,00	$ 426.267.501,00	32%	$ 199.999.999,00	2,5%
		Mejoramiento de la plataforma tecnológica del SUI que soporta los sistemas de información de la entidad	$ 1.000.000.000,00	$ 1.000.000.000,00	0%	$ 895.500.000,00	$ 104.500.000,00	90%	$ 895.500.000,00	11,2%
		OBJETIVO 2	$ 3.800.000.000,00	$ 3.700.000.000,00	-3%	$ 3.048.538.002,99	$ 651.461.997,01	82%	$ 3.017.744.668,99	37,6%
Modernizar y mantener actualizada la plataforma tecnológica de la entidad.	Licencias para Plataforma tecnológica	Adquirir y/o renovar el licenciamiento de cada una de las aplicaciones utilizadas en la entidad.	$ 1.541.307.645,00	$ 1.541.307.645,00	0%	$ 1.525.975.819,50	$ 15.331.825,50	99%	$ 628.678.041,50	7,8%
	Licencias de Ofimática	Adquirir e instalar las licencias de Ofimática (Windows, Call y Office) en los equipos de cómputo de la entidad.	$ 100.000.000,00	$ 100.000.000,00	0%	$ 38.304.629,11	$ 61.695.370,89	38%	$ 38.304.629,11	0,5%
	Equipos y elementos informáticos	Adquirir e instalar equipos de cómputo y elementos informáticos para uso de la entidad	$ 450.000.000,00	$ 370.000.000,00	-18%	$ 281.389.077,79	$ 88.610.922,21	76%	$ 0,00	0,0%
	Documentación para el Plan Estratégico	Documentar el plan estratégico de tecnologías de la información de la Oficina de Informática	$ 100.000.000,00	$ 100.000.000,00	0%	$ 90.516.000,00	$ 9.484.000,00	91%	$ 90.516.000,00	1,1%
		OBJETIVO 3	$ 2.191.307.645,00	$ 2.111.307.645,00	-4%	$ 1.936.185.526,40	$ 175.122.118,60	92%	$ 757.498.670,61	9,4%
Prevenir perdidas de información ante situaciones de desastre	Plan de Contingencia	Implementar los servicios del Centro de Datos Externos para la Superservicios	$ 571.768.219,00	$ 571.768.219,00	0%	$ 420.278.453,49	$ 151.489.765,51	74%	$ 420.278.453,49	5,2%
		Adecuar y/o implementar centro de datos	$ 1.606.924.136,00	$ 1.606.924.136,00	0%	$ 1.605.300.581,00	$ 1.623.555,00	100%	$ 963.180.348,00	12,0%
		OBJETIVO 4	$ 2.178.692.355,00	$ 2.178.692.355,00	0%	$ 2.025.579.034,49	$ 153.113.320,51	93%	$ 1.383.458.801,49	17,3%
		TOTALES	**$ 8.200.000.000,00**	**$ 8.020.000.000,00**	**-2%**	**$ 7.039.452.803,88**	**$ 980.547.196,12**	**88%**	**5.187.852.381,09**	**64,7%**

Durante la Vigencia 2017, se identifica una ejecución de recursos equivalente a ($7.039.452.803,88), es decir una ejecución del 88%, avanzando en ocho (8) productos, tal como se identifica a continuación:

Producto No.1

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Implementar y mantener actualizado un sistema de seguridad de la información, que proteja las redes de la entidad de riesgos informáticos.	Plataforma tecnológica de seguridad de la información	Plataforma tecnológica de seguridad de la información Mejorada	**100%**	**20%**	**20%**	**100%**	**80%**	**80%**

Observación 18: Se observó que se registró un avance del 20%, para las actividades programadas, tal como, la instalación de los certificados digitales SSL (Secure Socket Layer) para los dominios web, durante la vigencia 2017; no obstante, se observa, que esta actividad ya considerada ejecutada no ha sido efectiva en razón a los ajustes que se han tenido que realizar en éste periodo 2018 y que corresponden a los cambios que se realizarán en la página web para el módulo de ORFEO.

Se identifica que se están reportando actividades dentro de la ejecución del proyecto, que no se están desarrollando en su totalidad, independientemente de los factores internos, externos y/o no previstos.

Producto No.2

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Desarrollar y mejorar los sistemas de información y aplicativos que soporten la adecuada prestación de los servicios a cargo de la entidad.	Aplicaciones y/o Módulos nuevos desarrollados o implementados	Aplicaciones y/o Módulos nuevos desarrollados o implementados Desarrollados	**63**	**13**	**13**	**100%**	**51**	**81%**

Se evidencia el reporte de las siguientes nuevas soluciones informáticas.

	Primer Semestre 2017
1.	TARIFARIO AA – CARGUE. Radicado: 20171600015743
2.	NUEVO SITIO WEB. Radicado: 20171600016143
3.	ESQUEMA MONITOREO. Radicado: 20171600036063
4.	REPORTES DE ESTRATIFICACION. Radicado: 20171600028773
5.	SIGEP. Radicado: 20171600012673
	Segundo Semestre 2017
6.	APOYO TECNOLÓGICO PARA SIMPLIFICACIÓN DE FORMATOS Y FORMULARIOS DE CARGUE DE INFORMACIÓN SERVICIO DE ASEO. Radicado 20171600021733 y sus anexos.
7.	APLICACIÓN PARA LA VERIFICACION TARIFARIA DE ASEO – NUSD. Radicado 20171600050313 y sus anexos.
8.	CONTROL DE LOCALIDADES – ZNI. Radicado 20171600062403 y sus anexos.
9.	APLICATIVO APROVECHAMIENTO. Radicado 20171600067843 y sus anexos.
10.	CARGUES PARA SEGUIMIENTO Y MONITOREO DE CONTRATOS DE ESP INTERVENIDAS Y EN LIQUIDACION. Radicado 20171600050333 y sus anexos.
11.	Mejoramiento de la plataforma tecnológica del SUI que soporta los sistemas de información de la entidad. Expediente 2017527150100501E, Contrato 501 de 2017.
12.	Fortalecer el Sistema de Información Geográfico para la Superservicios. Expediente 2017527150100562E, Contrato 562 de 2017.
13.	Actualizar el sistema Business Process Management - BPM de la SUPERSERVICIOS. Expediente 2017527150100818E, Contrato 818 de 2017.

Producto No.3

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Desarrollar y mejorar los sistemas de información y aplicativos que soporten la adecuada prestación de los servicios a cargo de la entidad.	Sistemas de información	Sistemas de información Actualizados	70	20	20	100%	50	71%

Durante la vigencia se realizaron las siguientes actualizaciones a los sistemas de información existentes de la entidad:

Primer Semestre 2017
1. DISTRIBUCION FÁBRICA DE REPORTES, 2. ACTUALIZACION APP CARGUE NIF, 3. ACTUALIZACION FORMATO GASTOS PARA CONTRIBUCIONES FC01, 4. ACTUALIZACION FORMATO DE REGISTRO DE CORREO PARA NOTIFICACIONES Y REPORTES 5. ACTUALIZACION INSPECTOR, 6. ACTUALIZACION BASE PARA LIQUIDACION DE CONTRIBUCIONES, 7. ACTUALIZACION DE REPORTES SUI – GLP, 8. ORFEO Consulta Certificada, 9. ORFEO Firma digital con TOKEN, 10. ORFEO Módulo correo electrónico, 11. SISGESTION, 12. RECURSOS FISICOS, 13. JBPM
Segundo Semestre 2017
14. CARGUE NIF. Radicado 20171600015753 y sus anexos, 15. HABILITADOR AUTOMATICO. Radicado 20171600050293 y sus anexos, 16. DICCIONARIO DE VARIABLES. Radicado No. 20171600053323 y sus anexos, 17. ESQUEMA CILINDROS. Radicado 20171600076033 y sus anexos, 18. ACTUALIZACION SITIO Web. Formulario Denuncias ciudadanas. Expediente No. 2017160020800006E. Radicado 20171600012673 Anexo 122 y 123. Radicado: 20171600015063 Anexo: Formulario web quejas y reposición contra fallo SAP. Radicado 20171600012673. Anexo 125 y 127. Aprobación: Radicado 20171600012673. Anexo 126 y 128. Actualización urgente AppServi, Micrositio Convocatoria Digital y RETO No 2 Máxima Velocidad. Radicado 20171600012673 Anexos 147,148 y 149, 19. VOCALES DE CONTROL. Expediente No. 2017160020800006E. Radicado 20171600012673. Anexo 089 y 090. Soporte aceptación de usuario: Expediente 2017160180100001E. Radicado 20171600015063 Anexo 0239, 20. Orfeo. Radicado No. 20171600019143 anexos: 68,70,82,83,91,92,114

Se reportan veinte (20) sistemas de información y la descripción de la información verificada, corresponden a actualizaciones de funcionalidades de los Sistemas de Información de Orfeo, SUI, JBP, Cuentas por Cobrar, Página Web, entre otros. Fortalecer el reporte de actividades en la línea de inversión del producto.

Producto No.4

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Modernizar y mantener actualizada la plataforma tecnológica de la entidad.	Licencias para la plataforma tecnológica	Licencias para la plataforma tecnológica Actualizadas	33	10	10	100%	24	73%

Se revisa los expedientes mediante los cuales se acredita la adquisición de las licencias relacionadas a continuación:

1. Servicio en la Nube de productos Oracle Developer para la gestión de la información de investigaciones de energía, por agregación de demanda en la tienda virtual del estado colombiano Servicio de licencia y almacenamiento de base de datos en la nube
2. Adquisición y Renovación de licencias de productos de ofimática (Microsoft)
3. Soporte extendido para SIGEP - HEINSOHN HUMAN GLOBAL SOLUTIONS SAS.
4. ACL Acceso y Soporte
5. Actualizaciones sobre el SIGME. Actualización de SIGME ISODOC y renovar soporte técnico del Software-SIGME.

6. Firewall y mitigador de ataques. Renovación del servicio de Soporte, Mantenimiento y Garantía hasta 31 de diciembre de 2018 de los Appliances de Seguridad Informática
7. WAF y balanceadores, renovación del servicio de Soporte, Mantenimiento y Garantía hasta 31 de diciembre de 2018 de los Appliances de Seguridad Informática y Balanceadores de Carga de la SUPERSERVICIOS.
8. Productos de Red hat, renovación del servicio de soporte mantenimiento y garantía de los appliance de seguridad informática de la Superservicios incluido servicio de actualización a la última versión estable y disponible de los mismos y la adquisición de servicios red hat Enterprise de acuerdo a lo señalado en el alcance de cada uno de los grupos3.
9. Adquisición del software Enterprise arquitect licencias concurrentes, instaladas en el servidor y el cliente en máquinas de la oficina de Informática, para atención a requerimientos de la estrategia de gobierno en línea GEL.
10. Licencias aplicadas en los servidores de base de datos Oracle.

Producto No.5 y 6

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Modernizar y mantener actualizada la plataforma tecnológica de la entidad.	Licencias de ofimática	Licencias de ofimática Adquiridas	2667	200	200	100%	2467	93%

Se revisa: Contrato 563-17 - Orden de compra 19072:

- ✓ Windows ServerCAL License/SoftwareAssurancePack Government OLP 1License NoLevel UsrCAL 1 Licencia por Usuario - 152 - U
- ✓ Sistema Operativo Windows Server - Windows ServerCAL SoftwareAssurance Government OLP 1License NoLevel UsrCAL 1 Licencia por Usuario - 400 - Und - R18-016.

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Modernizar y mantener actualizada la plataforma tecnológica de la entidad.	Equipos y elementos informáticos.	Equipos y elementos informáticos. Adquiridos	444	35	35	100%	374	84%

Se revisa el Contrato 839-2017 -Summimas - Orden de compra 21833 y Contrato 883-2017. Adquisición de impresora de carnets (1 Unidad). La compra realizada de las impresoras y escáner adquiridos ascienden a 102 elementos, sin contar kit de mantenimientos.

Observación 19. A partir de la información suministrada por la Oficina de Tecnologías de la Información y la revisión realizada a los contratos, se observa una diferencia en la cantidad de licencias informadas (152 licencias nuevas más 400 renovadas) con las reportadas en el sistema de información SPI (200 licencias) y se identifica una diferencia en la cantidad de equipos y elementos informáticos adquiridos (102 elementos) con los reportados en el sistema de información SPI (35). Se identifica que no hay concordancia en la información.

Producto No.7

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Modernizar y mantener actualizada la plataforma tecnológica de la entidad.	Documentación para el plan estratégico	Documentación para el plan estratégico Formulado	1	1	1	100%	1	100%

La Oficina de Tecnologías de la información, argumenta que la formulación del Plan Estratégico se llevó a cabo bajo el contrato 486 de 2017 (Expediente ORFEO 20175271501004 86E), suscrito con Hernando José Peña Villamil, el cual tiene por objeto: "Prestar sus servicios profesionales para apoyo en las actividades de actualización del Plan Estratégico de TI a cargo de la Oficina Informática". Los resultados de dicha contratación, se encuentran en el Radicado 20171600016483, anexos, 0052, 0070, 0072, 0073, 0074, 0087, 0088, 0101, 0132, 0136, 0138, 0139, 0140 y 0141.

Observación 20. Bajo el desarrollo del proyecto de inversión, en el Producto "Documentación para el Plan Estratégico", se identifica la entrega del documento denominado "ACTUALIZACIÓN PLAN ESTRATÉGICO DE TI - SSPD 2018-2020", el cual, comprende los contenidos globales establecidos por MinTIC, como criterios mínimos para la construcción del PETI, del cual se identifica por complementar, los componentes que corresponden a: Entendimiento Estratégico, Modelo de Gestión y Modelo de Planeación.

En el documento de Actualización Plan Estratégico de TI, falta integrar los resultados obtenidos en el ejercicio de Arquitectura Empresarial, trabajado con la Universidad Nacional bajo el Contrato No. 501 de 2017, el cual tenía por objeto *"Diagnosticar, definir y Diseñar la Arquitectura Empresarial asociada con los procesos misionales de la Superintendencia de Servicios Públicos Domiciliarios, para alinear el Sistema Único de Información SUI – con los aspectos estratégicos, operativos y organizacionales de la Entidad"*; dado que no se documentan las Arquitecturas para Información, Sistemas de Información, Infraestructura Tecnológica.

De lo anterior, y bajo el reporte efectuado en el proyecto de inversión, se concluye que el documento requiere completar los componentes, arriba enunciados. Se reitera de igual forma las observaciones emitidas bajo el informe de auditoría TIC con radicado 20171400102603 y el informe de Gobierno en Línea con radicado 20171400054023.

Producto No.8

Objetivos Específicos	Producto	Indicador	PRG 2013-2018	Meta Vigente 2017	Avance SPI 2017	% Eje 2017	Avance Acumulado 2013-2018	% Ejecución Acumulado 2013-2018
Prevenir perdidas de información ante situaciones de desastre	Plan de Contingencia	PLAN DE CONTINGENCIA Implementado	100%	20%	20%	100%	71%	71%

Observación 21. El avance acumulado de Plan de Contingencia para la Vigencia 2017 es del 71%, el cual se encuentra respaldado en las actividades (Implementar los servicios del Centro de Datos Externos para la Superservicios, Servicios del centro de datos externos en funcionamiento y Sostenibilidad del servicio de centro de datos externos), no es visible documentalmente. Igualmente, el contrato 819 de 2017, con el proveedor Infotic, establece la elaboración y mantenimiento de un plan de contingencia dentro del alcance del contrato, así como la elaboración de un plan de recuperación de desastres (DRP), los cuales se encuentran comentados en la observación 15.

2.1.5.3. Metodología de Seguimiento de Proyecto de Inversión Oficina TIC

Se identifica que durante la vigencia 2017, la Oficina de Tecnologías de la Información, adoptó un esquema de seguimiento propio para controlar el desarrollo y avance del proyecto de inversión; bajo éste modelo interno, se desarrollaron las siguientes acciones:

Metodología de Seguimiento TIC – Vigencia 2017	Observaciones y Recomendaciones OCI
1. Diligenciamiento de Matriz de Seguimiento para el cumplimiento del PAA y el PAC institucional	
El Grupo de Tecnologías de la información, diligencia la matriz de seguimiento del Plan Anual de Adquisiciones - PAA y el Plan Anual de Caja - PAC del Proyecto de Inversión. (Método definido por la Oficina de Planeación para controlar el cumplimiento del PAA y del PAC respectivamente.	Se verifica con el Profesional Diego Mauricio Moreno de la Oficina Asesora de Planeación, la realización de una metodología para hacer seguimiento presupuestal en comparación con el PAC y PAA, la cual está en proceso de implementación para los proyectos 2018 y con un análisis de impacto a 31 de diciembre de 2017, el cual incluye el proyecto "Fortalecimiento de los Sistemas de Información en la Superintendencia de Servicios Públicos Domiciliarios". Se recomienda que este esquema unificado de seguimiento se formalice bajo el desarrollo del Proceso de Direccionamiento Estratégico DE-PR-001 – Procedimiento Gestión de Proyectos de Inversión DE-P-001.
2. Matriz de Seguimiento Presupuestal 2017	
La Oficina de Tecnologías de la Información, adopto internamente una matriz de seguimiento mediante la cual controlo las siguientes variables: Números de Contrato, Nombre de Contratistas, Fuente de Financiación Contrato No., Actividad Asociada del Proyecto, Valor Inicial CD, Valor Real Contrato, Valor luego de Novedad, Valor a Liberar, Valor Luego de la Novedad, Valor a Liberar, Tiempo meses, Tipo de contrato, Observación, Valor Pago Mensual, Valor Pagado, N. de Pago, Saldo por Ejecutar, Valor CDP adición, Fecha de Inicio, Fecha Final, Supervisor, Número CRP, Número CDP, Número PAA, Fecha de pago informe actividades. Durante la vigencia 2018, se unifico en la matriz los criterios mencionados, adicionando el presupuesto obligado para cada proceso de contratación.	Se identificó para el cierre de la vigencia 2017, que se encontraban dos (2) matrices con los mismos datos; sin embargo, una de las matrices contenía los datos de Contratos Obligados y la otra no, por lo cual se hizo necesario verificar en las dos matrices la conciliación de saldos presupuestales para obligaciones y pagos. Al respecto se recomienda: Que se ejerzan acciones de verificación y seguimiento sobre los ítems relacionados a continuación, dadas las acciones de control requeridas en el ejercicio de seguimiento presupuestal que ameritan los Proyectos de Inversión. **Items:** Objetivo Específico, Meta (Producto), Actividad, Id Proyecto- Id Actividad, Tipo de contrato, Objeto contractual Propuesto, Cantidad de Bienes o servicios estimados a comprar, Clasificación de Costo por PAA, Fuente de Financiación, Valor unitario (Mes), Plazo de ejecución (Meses), Presupuesto Asignado, Valor anterior, Presupuesto Comprometido a la fecha (Registros), Saldo por Comprometer, Procesos en curso (CDP por comprometer), Fecha proyectada de contratación, Modalidad de selección, Justificación del cambio, Fecha de modificación, No. Contrato, Forma de Pago, Nombre contratista, No. Identificación, Supervisor, CDP, VALOR CDP, No. CRP, VALOR CRP, SALDO CDP Vs CRP, Fecha de CRP, Fecha de inicio, Fecha de terminación, Requiere Acta de Liquidación, Estado de contratación. **PRESENTACIÓN CUENTAS**, Compromisos por Mes (Ejemplo Ene, Feb. Mar, etc.), % Avance Compromisos, Pago Programado por Mes, Pago Ejecutado o Pagado, Saldo del mes, % Giros del mes, % Giros Apropiación (Disponible). **TOTAL, PAGOS PROGRAMADOS VIGENCIA,** Total, Pagado, Saldo, % Giros Vigencia, % Giros Total Apropiación (Disponible), Cuenta por Pagar, Reserva (En caso de Requerirse con Justificación), Monto por Ejecutar (Pagos) Vigencia Este ejercicio puede generar valor agregado en torno a gráficos comparativos y estadísticas que muestren y alerten el comportamiento periódico del proyecto tanto en recursos presupuestales como en avance de productos. Se recomienda de igual forma, que las acciones de control sean definidas institucionalmente, de tal manera que la Entidad aborde un esquema unificado sobre el seguimiento presupuestal del Proyecto de Inversión y que éste esquema consolide los mismos criterios o parámetros de seguimiento.
3. Solicitud de Información mensual al Área Financiera, con respecto a los reportes de SIIF	
La información de reportes SIIF, se solicita por correo por parte del profesional encargado de seguimiento al proyecto y se recibe por la misma vía; una vez se recibe el reporte, se concilia la información con la matriz de seguimiento presupuestal adoptada internamente.	Se identifica como fortaleza este ejercicio de conciliación de cifras para el seguimiento de ejecución presupuestal (Certificados y registros Presupuestales), así como causación de pagos del proyecto. Se recomienda formalizar éste tipo de prácticas para el seguimiento de todos los proyectos de inversión de la Entidad.

4. Seguimiento de Avance de Productos y Actividades	
El reporte de avance de productos, es registrado directamente en SPI, y se consolidan en el informe ejecutivo, el cual se carga de igual forma en el aplicativo SPI. La información se solicita por correo.	Se identifican debilidades en este aspecto, dado que, las evidencias de los productos no se van consolidando en el cierre de cada periodo (Mensual), no se cuenta institucionalmente con un esquema unificado de seguimiento de productos. Estas debilidades se ven reflejas en las observaciones emitidas por cada producto. Se recomienda, que se implemente un método de seguimiento, mediante el cual los responsables por producto, acrediten mensualmente, tanto el avance porcentual como cualitativo de ejecución y a través del cual, también se recopilen las evidencias de las cantidades reportadas en los periodos de ejecución.

3. CONCLUSIONES

Se destaca el trabajo que se realiza en la construcción del catálogo de información de la base de datos SUI, la cual articula de forma automática la norma, los formatos y formularios de la norma, el diccionario de datos, la base de datos y la publicación de la norma y la tecnología involucrada en el proceso.

Se referencia el acompañamiento de apoyo que ha efectuado el equipo de gestión de tecnología, en lo relacionado a la publicación de datos abiertos del sector de energía y gas combustible, para dar cumplimiento a los lineamientos establecidos en la ley de transparencia.

Se señala la adecuación física al centro de datos, en la sede de la Cll 84, la cual le permite tener un mejor control periférico y del centro de control de la red, así como de la distribución y organización interna de los equipos de procesamiento y comunicaciones

Se observan algunas debilidades, como las citadas a lo largo del informe, en el proceso de Gestión Tecnologías de la Información, para las cuales es necesario implementar correctivos que permitan mitigar los riesgos que se puedan derivar de las situaciones manifestadas en cada subproceso, tales como:

- Sistema Único de Información, lo referente a: administración de contraseñas, gestión de usuarios, registro de cambios de parámetros de usuario y publicación instructivos de estructura de datos y archivos de cargue.

- Desarrollo de Soluciones Informáticas, pertinente a: verificación y ejecución de pruebas no funcionales de software, desarrollo metodológico del ciclo de vida de los sistemas de información.

- Gestión y Operación de la Infraestructura Tecnológica, en cuanto a: transporte de software al ambiente de software, gestión de cambios, gestión del registro versión de software, seguimiento mesa de servicios y gestión de proveedores.

RECOMIENDACIONES

1. Es conveniente desarrollar la declarativa de seguridad y privacidad de la información, en lo referente a realizar pruebas de aceptación de los sistemas nuevos y en mantenimiento, gestionar los cambios de versiones, incluyendo las pruebas definidas como "no funcionales", en los procedimientos internos.

2. Efectuar en el ambiente computacional de pruebas, el proceso y ejercicio de pruebas de software, para reducir riesgos de acceso o cambios no autorizados en la operación.

3. Evaluar el ciclo metodológico del desarrollo de soluciones informáticas, con el fin de tener en cuenta los lineamientos de arquitectura TI, plan estratégico TI, arquitectura de sistemas de información, arquitectura de información, servicios tecnológicos, estrategia de uso y apropiación.

4. Definir e implementar mecanismos de ciframiento seguros y ágiles que protejan las claves de los usuarios de las empresas prestadoras de servicios que acceden el sistema SUI.

5. Evaluar la lista de usuarios que ingresan por el sistema de autenticación SUI o por el la base de datos, con el fin de fortalecer los mecanismos de control referentes a la administración y gestión de usuarios.

6. Evaluar las consultas que realizan los usuarios a la base de datos SUI, con el fin de implementar soluciones automáticas y trazables en la plataforma del sistema.

7. Implementar de forma controlada y segura la solución informática para el trámite automático de habilitaciones, retiros y reversiones de formatos y formularios, a través de la mejora del habilitador automático.

8. Desarrollar mecanismos de trazabilidad y registro de las operaciones que realizan los usuarios en el aplicativo o base de datos, tanto para usuarios internos como prestadores de servicio, con el fin de supervisar las actividades no autorizadas.

9. Fortalecer actividades de supervisión en la gestión de cambios, versiones y configuración, además, propender por herramientas automáticas para el control del despliegue de software productivo.

10. Implementar las acciones de control recomendadas para el mejoramiento de la "Metodología de Seguimiento de Proyecto de Inversión Oficina TIC", enunciadas en el numeral 2.1.5.3.

11. Estructurar el Plan Estratégico de Tecnologías de la Información, fortaleciendo su contenido, bajo la integración de los resultados de Arquitectura Empresarial en torno al Entendimiento Estratégico, definir la Arquitectura de TI para enfocar el Modelo de Gestión que adoptara la Oficina de Tecnologías de la Información y desarrollar el Modelo de Planeación mediante el cual se estructuren las actividades y proyectos (recursos presupuestales, de infraestructura, técnicos y operativos) del PETIC, desarrollados bajo el seguimiento y control del Mapa de Ruta que se defina para su ejecución.

Es preciso recordar que, la aplicación de las recomendaciones emitidas por la Oficina de Control Interno, queda sujeta a la discrecionalidad del líder del proceso, ya que pueden determinarse otras acciones correctivas, preventivas o de mejora, para eliminar las situaciones detectadas en la auditoría que afectan la debida gestión del proceso.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Cargo**	**Firma**
Myriam Herrera Durán	Jefe Oficina Control Interno	