



OCI

20221350445913

Información Pública

Al responder cite este número

FECHA: Bogotá D.C., diciembre 28 de 2022

PARA: **Gian Carlo Suescún Sanabria**
Director General (e)

DE: Jefe Oficina de Control Interno

REFERENCIA: Informe final de auditoría al Proceso de Gestión de Tecnologías de Información y Comunicación 2022

Respetado doctor Gian Carlo:

Reciba un cordial saludo. Como parte del Plan Anual de Auditoría para la vigencia 2022 y en cumplimiento de las disposiciones contenidas en el Decreto 648 de 2017 y el Decreto Distrital 807 de 2019 en relación con el destinatario principal de los informes de auditoría, seguimientos y evaluaciones, en su calidad de representante legal, remito el Informe final de auditoría al Proceso de Gestión de Tecnologías de Información y Comunicación 2022, el cual se informa a la Oficina Asesora de Planeación – OAP, según solicitud efectuada mediante memorando 20171150244353; y a la Subdirección General de Gestión Corporativa, a la Dirección Técnica Administrativa y Financiera y a la Subdirección Técnica de Recursos Tecnológicos, como dependencias líderes del proceso.

Los hallazgos relacionados en el informe adjunto corresponden a la evaluación de parte de la muestra definida para la auditoría, por lo cual es importante que, desde las dependencias/procesos involucrados, se efectúe una revisión de carácter general sobre los aspectos evaluados.

Es necesario que las dependencias responsables formulen, a partir de los hallazgos evidenciados, un plan de mejoramiento que contenga las acciones pertinentes para subsanar la raíz de las deficiencias encontradas, conforme con lo establecido en el procedimiento PR-MC-01 "Formulación, Monitoreo y Seguimiento a Planes de Mejoramiento", V.10.

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 400 de marzo 11 de 2021

1



OCI

20221350445913

Información Pública

Al responder cite este número

Para elaborar el plan de mejoramiento se debe emplear el formato FO-MC-01 “*Plan de Mejoramiento*”, versión 7.0, y es necesario diligenciar uno o varios de los instrumentos de análisis de causas que se encuentran dentro del mismo.

De acuerdo con lo establecido en el procedimiento mencionado, las dependencias responsables cuentan con ocho (8) días hábiles, a partir del día siguiente al recibo de este informe, para la presentación del plan de mejoramiento resultado de la evaluación.

Es necesario aclarar que, dada la declaratoria de ineffectividad de las acciones de mejoramiento 2522 y 2523, el plan de mejoramiento que se formule debe incluir, también, una o más acciones, diferentes a las mencionadas, que permitan eliminar la(s) causa(s) de los hallazgos o no conformidades inicialmente detectados.

La Oficina de Control Interno agradece la colaboración que se ha prestado para el desarrollo de la presente auditoría y reitera su disposición para brindar la asistencia y acompañamiento requeridos, conforme a sus roles y funciones.

Cualquier información adicional, con gusto será atendida.

Cordialmente,



Ismael Martínez Guerrero

Jefe Oficina de Control Interno

Firma mecánica generada en 28-12-2022 06:51 PM

Anexos: - Informe final auditoría al Proceso de Gestión de Tecnologías de Información y Comunicación 2022.
- Anexo N.º 1 Análisis de riesgos de gestión y corrupción – Gestión de TIC.
- Anexo N.º 2 Debilidades en tiempos de atención (ANS), Casos agosto 2022.

cc Hector Pulido Moreno - Subdirección Técnica de Recursos Tecnológicos
cc Mercy Yasmin Parra Rodríguez - Subdirección General de Gestión Corporativa
cc Mercy Yasmin Parra Rodríguez - Dirección Técnica Administrativa y Financiera

Elaboró: Adriana Mabel Niño Acosta - Oficina de Control Interno

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

1. INFORMACIÓN GENERAL

Tipo de Informe	Preliminar <input type="checkbox"/>	Final <input checked="" type="checkbox"/>	Fecha elaboración de informe:	de del 28/12/2022
Proceso/Objeto Auditado	Auditoría interna al proceso de Gestión de Tecnologías de Información y Comunicación			
Líder del proceso/ Cargo y dependencia	Rosita Esther Barrios Figueroa - Subdirectora General de Gestión Corporativa			
Líder operativo del Proceso/ cargo y dependencia	Mercy Yasmín Parra Rodríguez – Directora Técnica Administrativa y Financiera Arleth Patricia Saurith Contreras – Subdirectora Técnica de Recursos Tecnológicos			
Tipo de Auditoría	Gestión			
Objetivo	Evaluar la gestión del proceso de Gestión de Tecnologías de Información y Comunicación, a través de la verificación del cumplimiento de la normatividad y directrices institucionales aplicables a algunas de las actividades críticas del mismo, a fin de identificar aspectos que contribuyan a su mejoramiento continuo.			
Alcance	<p>La auditoría tuvo como alcance la verificación de soportes, registros y documentación asociada con las actividades críticas establecidas en la caracterización del proceso de Gestión de Tecnologías de Información y Comunicación (Gestión de TIC):</p> <ul style="list-style-type: none"> • Actividad crítica “1. <i>Direccionamiento estratégico de TIC</i>”. Productos “1. <i>Plan Estratégico de Tecnologías de la Información– PETI</i>”, “2. <i>Plan de adquisiciones TI / Plan de contratación TI</i>”, “4. <i>Indicadores de Gestión del proceso</i>” y “5. <i>Matriz de riesgos institucionales proceso</i>”. • Actividad crítica “2. <i>Administración de Infraestructura de T.I.</i>”. Productos “2. <i>Gestión de capacidad</i>”, “3. <i>Copia de respaldo ordinaria</i>”, “4. <i>Copia de respaldo por demanda</i>” y “5. <i>Información restaurada</i>”. • Actividad crítica “5. <i>Soporte a los Servicios de TI</i>”. Productos “1. <i>Registro del evento, incidente, problema o requerimiento atendido, solucionado y cerrado</i>” y “2. <i>Informe del prestador del servicio</i>”. • Actividad crítica “9. <i>Seguimiento a la Gestión</i>”. Productos “1. <i>Análisis de la evaluación del servicio</i>”, “3. <i>Indicadores de gestión del proceso analizados</i>”, “4. <i>Informe de seguimiento a las acciones de mejora en curso a cargo del proceso</i>”, “5. <i>Informe de seguimiento a riesgos del proceso</i>” y “6. <i>Informe de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS</i>”. <p>Las actividades de auditoría se basaron en la verificación de información suministrada por el proceso (entregada en medio físico, digital y/o entrevistas), la información consultada en sistemas de información aplicables al proceso y</p>			

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

	entrevistas, entre otras actividades. La evaluación se realizó con base en la gestión adelantada entre el 01/01/2022 y el 30/09/2022.
Criterios de Auditoría	<ul style="list-style-type: none"> • Normograma IDU vigente para el proceso. • Documentación del Sistema de Gestión MIPG-SIG y demás documentación publicada en la intranet, aplicable al proceso. • Sistemas de información aplicables o relacionados con el proceso (Sistema de Información y Acompañamiento Contractual – SIAC, Sistema de Gestión Documental, Sistema de Gestión Mesa de Servicios TI – Aranda, Sistemas de Apoyo a la Gestión Administrativa CHIE y/u otros). • Matrices de riesgos y planes de tratamiento a los mismos, del proceso de Gestión de Tecnologías de Información y Comunicación. • Plan Anual Estratégico – PAE. • Indicadores reportados en el <i>Balanced Scorecard</i>, publicados en la Intranet y la página web y aplicables al periodo a evaluar. • Planes de mejoramiento interno vigentes.
Fecha reunión de apertura	12/10/2022
Fecha reunión de cierre	21/12/2022
Equipo auditor/ Dependencia/ Rol	Adriana Mabel Niño Acosta – Profesional Especializado 222-05 – Auditor Líder Camilo Oswaldo Barajas Sierra – Profesional Especializado 222-05 – Auditor Fernando Garavito Guerra – Profesional Especializado 222-04 – Auditor

2. METODOLOGÍA

De acuerdo con el Plan de Auditoría, remitido mediante el memorando 202213500350593 del 10/10/2022, y los alcances, remitidos mediante memorandos 20221350394723 del 22/11/2022 y 20221350424423 del 14/12/2022, la auditoría fue desarrollada entre el 13/09/2022 y el 21/12/2022, periodo en el cual el equipo auditor realizó la planeación y ejecución de la auditoría al proceso de Gestión de Tecnologías de Información y Comunicación.

La auditoría se llevó a cabo a través de entrevistas virtuales, visitas *in situ* y la verificación de la información suministrada por el proceso (entregada en medio magnético o presentada en las entrevistas), la información consultada en sistemas de información institucionales o externos, entre otras actividades. La evaluación se realizó sobre la gestión adelantada por el proceso, principalmente, durante la vigencia 2022 con corte al 30/09/2022; no obstante, se realizaron consultas relacionadas con el Plan Estratégico de Tecnologías de Información (PETI) que abarcaron 2021, así como consultas de información que fueron posteriores al 30/09/2022, como es el caso de usuarios de red.

Para el logro del objetivo de la auditoría, se realizaron entre otras, las siguientes actividades:

- Revisión de la documentación asociada al proceso publicada en la intranet institucional y en SUE: Sistema de Información Documentada.
- Entrevistas a los funcionarios que hacen parte del proceso evaluado, con el propósito de que aportaran la información y/o documentación, así como precisar o aclarar las inquietudes del equipo auditor.

FORMATO		
INFORME DE AUDITORIA		
CÓDIGO	PROCESO	VERSIÓN
FO-EC-111	EVALUACIÓN Y CONTROL	1.0



- Consulta de información asociada al proceso o para consulta de información relevante y necesaria y ubicada en sistemas de información como SIAC, ORFEO, SECOP II, CHIE: Plan Mejoramiento Institucional, CHIE: Gestión TIC, Aranda, entre otros.

Los registros revisados correspondieron a información aportada por la Subdirección Técnica de Recursos Tecnológicos - STRT, la Subdirección Técnica de Recursos Humanos - STRH y la Oficina Asesora de Planeación - OAP, relacionada con las actividades críticas enunciadas en el alcance de la auditoría.

A continuación, se relacionan los aspectos evaluados por cada una de las actividades críticas y temáticas relacionadas en el alcance de la auditoría, atendiendo los productos descritos en la caracterización del proceso de Gestión de Tecnologías de Información y Comunicación.

- Actividad crítica “1. *Direccionamiento estratégico de TIC*”.

Las pruebas de auditoría aplicadas al tema se basaron en la verificación del cumplimiento de los estándares establecidos en la Guía del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) G.ES.06 Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI, versión 1.1 de octubre de 2019, así como el cumplimiento de las metas de contratación de acuerdo con el PETI.

También se realizó una revisión del *Plan de adquisiciones TI / Plan de contratación TI*.

De otra parte, se revisaron las matrices de riesgos de gestión y corrupción que administra el proceso, a las cuales se aplicaron pruebas de coherencia, verificación de los controles y de sus registros.

- Actividad crítica “2. *Administración de Infraestructura de T.I*”.

Las pruebas de auditoría aplicadas al tema se basaron en la verificación del cumplimiento de aspectos relacionados con la Gestión de capacidad y la generación y restauración de copias de respaldo. Para ello, se realizaron entrevistas virtuales, se solicitaron registros y se verificaron asuntos en las herramientas de la STRT.

- Actividad crítica “5. *Soporte a los Servicios de TI*”.

Las pruebas de auditoría aplicadas al tema se basaron en la verificación del Registro de casos de requerimientos de soporte de TI en la herramienta Aranda, verificación del cumplimiento de los acuerdos de niveles de servicio, así como una revisión para el uso de la herramienta de gestión de usuarios. Para ello, se realizaron entrevistas virtuales, se solicitaron registros, se hicieron cruces de información, entre otras.

- Actividad crítica “9. *Seguimiento a la Gestión*”.

Las pruebas de auditoría aplicadas al tema se basaron en la verificación de los resultados de los indicadores del proceso y de las acciones incluidas en el Plan de Acción Estratégico (PAE), a través de entrevistas virtuales, visita a la sede de la STRT, verificación de la información suministrada por el proceso y la consultada en sistemas de información o herramientas como el tablero de control o *Balanced Scorecard* institucional.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

También se llevó a cabo un análisis de efectividad de las acciones de mejora en estado terminado, para pronunciamiento de efectividad. En relación con el seguimiento a riesgos del proceso se verificaron la oportunidad en el reporte y los casos de materialización reportados.

Por último, se verificó el producto “Informe de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS”.

3. RESULTADOS DE LA AUDITORÍA

A continuación, se presentan los resultados del ejercicio de evaluación adelantado por el equipo auditor para cada una de las actividades críticas descritas:

Actividad crítica 1. Direccionamiento estratégico de TIC.

De acuerdo con la caracterización del proceso de Gestión de Tecnologías de Información y Comunicación (Gestión de TIC), esta actividad crítica busca, entre otros aspectos el “Definir la planeación estratégica de Tecnologías de Información del IDU, a partir del análisis y diagnóstico de tecnologías existentes y las necesidades identificadas en los usuarios. [...]”. Algunas de las salidas o productos de esta actividad que se abordaron en esta auditoría son el Plan Estratégico de Tecnologías de la Información– PETI, el Plan de adquisiciones TI / Plan de contratación TI, el Plan de Acción Estratégico (PAE) del proceso y la definición de Indicadores y Matriz de riesgos institucionales del proceso.

A continuación, se presenta la información correspondiente frente a cada uno de los productos revisados como parte del análisis de esta actividad crítica:

1. Plan Estratégico de Tecnologías de la Información– PETI

Se adelantó la revisión del Plan Estratégico de Tecnologías de la Información, para lo cual se empleó como criterio la Guía establecida por el Ministerio de Tecnologías de Información y Comunicaciones de Colombia, G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI, versión 1.1 de octubre de 2019.

Al respecto, se pudo verificar que este modelo fue el empleado por la Subdirección Técnica de Recursos Tecnológicos – STRT para elaborar el PETI 2021-2024 del Instituto de Desarrollo Urbano – IDU.

Se aclara que el equipo auditor tuvo conocimiento de la elaboración y aprobación del PETI V15 a finales de noviembre de 2022, pero para este ejercicio auditor su empleo fue solamente informativo, por cuanto la fecha de su aprobación excede los límites de la auditoría.

Al respecto se realizan las siguientes observaciones:

Frente al alcance, es importante establecer que el PETI es Institucional, es decir, la expresión que se realiza en el documento del IDU no debe corresponder a la contribución de la STRT, sino al compromiso institucional en materia de Tecnología de la Información. Se verificó que a la fecha se han adelantado por lo menos dos etapas de las planeadas de Arquitectura Empresarial (AE), situación que es necesario se integre a este documento. La Guía G.ES.06 expresa: “El PETI hace parte integral de la estrategia de la

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI. Cada vez que una institución pública hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI”. Adicionalmente, es claro para la institución el alcance del PETI, toda vez que su aprobación no se da en el interior de la STRT, sino en un órgano colegiado como es el “Comité de Gestión y Desempeño”. Lo que ratifica que es un elemento de estrategia institucional.

De otra parte, la guía es clara al establecer que “Se describe claramente el alcance del PETI teniendo en cuenta que debe proyectarse a máximo cuatro años y debe actualizarse cada año. El alcance del PETI debe indicar lo que efectivamente debe lograr la entidad durante la vigencia del PETI. El alcance establecido en el PETI debe dar cubrimiento a todos los dominios del Marco de Referencia de AE”. El alcance descrito en el documento PETI IDU 2021-2024, que a la letra expresa: “Este documento contiene las estrategias y lineamientos que ejecutará la Subdirección Técnica de Recursos Tecnológicos durante los años 2021 - 2024, para contribuir en el cumplimiento de las funciones de la Entidad y en el logro de los objetivos institucionales” limita su alcance a detallar la vigencia 2021 y de manera general esboza las vigencias 2022 y 2023, pero no indica lo que efectivamente debe lograr la entidad durante la vigencia del PETI, por lo que no sigue con rigor el lineamiento descrito en la Guía.

Con respecto a los objetivos, el único que se plantea no es medible y no permite cuantificar el proceso que se adelantará con el desarrollo del PETI. Se recomienda definir objetivos específicos más explícitos que permitan su adecuado seguimiento. De otra parte, la inclusión en el objetivo de la expresión “[...] en respuesta a las necesidades de la Entidad, sus objetivos misionales, los lineamientos estratégicos institucionales y la normatividad y estándares vigentes sobre Gobierno Digital, Transformación Digital e Innovación” corresponde a la definición de los requisitos que para este componente define la Guía, por lo que se estima que su transcripción no se requiere en este documento. En este sentido se recomienda adaptar los lineamientos establecidos en la Guía G.ES.06 Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI a la casuística del IDU, evitando la transcripción literal de algunos contenidos de la misma en temas relevantes como el objetivo del PETI.

El Marco Normativo no se encuentra actualizado para la fecha de elaboración del documento, por cuanto no se contempló la modificación de la estructura organizacional correspondiente al Acuerdo 02 del 25 de enero de 2017. Adicionalmente, se debe tener en cuenta que este tipo de documento, en el Marco Normativo, debe mantener una estructura que responda a la denominada pirámide de Kelsen¹ y mantenga el orden cronológico.

Con respecto a las “Rupturas Estratégicas”, no fue posible determinar la metodología de su formulación, por cuanto al indagarse acerca de ellas, el personal entrevistado solamente hizo referencia a las necesidades y oportunidades de mejora en servicios y trámites, pero no a las rupturas estratégicas. De igual manera, el proceso no tiene claridad acerca de los paradigmas que se están rompiendo o superando y en el documento no se aprecia el empleo de este elemento para la definición del PETI 2021-2024.

Frente al numeral 6. ENTENDIMIENTO ESTRATÉGICO, están registrados el modelo operativo de la actual administración, el mapa de procesos, pero no se desarrolla algún tipo de análisis a partir de esta información, lo cual debe entenderse como una oportunidad de mejora del documento, toda vez que este tipo de análisis sustenta la definición de las oportunidades y brechas que se describen en otras partes del documento. Se recomienda desarrollar este capítulo en concordancia con el capítulo 7. ANÁLISIS DE LA SITUACIÓN ACTUAL. Se debe tener en cuenta que la finalidad del PETI es definir la estrategia de la

¹ <https://www.studocu.com/document/universidad-externado-de-colombia/derecho-constitucional/piramide-de-kelsen-colombia-laura-guzman/16614600>

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

entidad en materia de Tecnología de la Información y Comunicaciones, por lo que su alcance podría ir más allá de las necesidades y capacidades de la dependencia que la gerencia, ampliando el espectro a las capacidades, necesidades y expectativas de y frente a la entidad.

Teniendo en cuenta que los ejercicios de Arquitectura Empresarial son insumo para mantener actualizado el PETI, se considera importante que en este último documento se relacionen las conclusiones de los documentos en los que se realizan los análisis o se realicen extractos de los mismos, debidamente referenciados, en los cuales se evidencien los análisis que fundamentan las modificaciones o mejoras que se propone adelantar. De acuerdo con lo evidenciado en la versión 14 del PETI, esta práctica no se está llevando a cabo.

El capítulo 7, ANÁLISIS DE LA SITUACIÓN ACTUAL, presenta información actual que corresponde al numeral 2.7 MODELO DE GESTIÓN DE TI de la Guía Técnica, que dice: *“Este numeral, describe el deber ser o la situación deseada en materia de gestión de TI, desde el punto de vista de cada uno de los dominios del Marco de Referencia de Arquitectura Empresarial.”* Es decir, para la Guía estos elementos: Estrategia de TI, Gobierno de TI, Gestión de información, Sistemas de Información, Modelo de gestión de servicios tecnológicos y Usos y apropiación, deben plantearse como una propuesta en esta sección, no registrarse como parte de la descripción de la situación actual.

El PETI – IDU, versión 14, expresa: *“Los objetivos estratégicos de TI representan el estado que la entidad quiere lograr o sostener en su Gestión TI a través de los medios adecuados para impulsar el fortalecimiento institucional. Así mismo, define los fines principales para avanzar hacia el cumplimiento de la visión de TI e institucional”* y menciona que, a enero de 2021, los siguientes eran los que ya se encontraban establecidos:

- “OE-01 Liderar las iniciativas del IDU desde una visión tecnológica, para dar cumplimiento a los objetivos institucionales y al plan de transformación digital con innovación, pensamiento estratégico y disciplinas ágiles.*
- OE-02 Fortalecer y mantener el Subsistema de Gestión de Seguridad de la Información, mediante la adopción de las mejores prácticas, la implementación de controles que mitiguen los riesgos y la apropiación de los conceptos de seguridad de la información por parte de la Gente IDU.*
- OE-03 Incorporar nuevas tecnologías que habiliten la transformación digital en los procesos, trámites y servicios de la Entidad, para fortalecer la eficiencia administrativa y generar valor público a los grupos de interés.*
- OE-04 Desarrollar estrategias de integración de información e interoperabilidad para soportar los requerimientos institucionales, interadministrativos y del sector con el uso de la tecnología”.*

Dado esto, el ejercicio de planeación efectuado con el PETI se torna parcial, por cuanto uno de sus elementos fundamentales, como es la definición de los objetivos, se realizó de manera previa al ejercicio al cual pertenece.

De otra parte, no es claro el empleo que se hizo de la información de los indicadores del proceso en las vigencias 2020 y 2021, tal como se registró en el PETI 2021, y su integración con la estructuración de las estrategias que se definen como producto de la planeación estratégica de TIC. La Guía Técnica establece frente a los indicadores: *“Para cada uno de los seis (6) dominios del plan maestro se deben definir indicadores de logro y resultado, incluyendo: tipo Indicador (proceso o logro), nombre, descripción, metas para los siguientes años, meta (valor esperado)”*, criterio que no se evidencia en la versión 14 del PETI – IDU, toda vez que no se elaboraron indicadores con esta característica.

Al revisar el “Plan Maestro o Mapa de Ruta”, se pudo verificar que, con respecto a la magnitud de las metas de los proyectos, el PETI no presenta información, salvo en los casos de los contratos de

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

mantenimiento o de consultoría, que en sí mismos son la unidad; los proyectos no presentan una cuantificación que se pueda identificar para determinar la magnitud de los mismos ni un criterio que permita determinar la magnitud de la brecha que se pretende superar con la aplicación de este plan.

Los proyectos se encuentran cuantificados en pesos y se presentan agrupados por “*necesidad y fuente del presupuesto: Proyectos Plan Anual de Adquisiciones, Proyectos Plan de Acción Estratégica y Proyectos de Transformación Institucional*”.

Particularmente, se registra la desagregación de los recursos de la vigencia presupuestal de 2021, por valor de \$ 28.105.599.000, correspondientes a los proyectos del Plan Anual de Adquisiciones 2021, del cual se tomó una muestra de 11 proyectos por valor cercano al 60 % de los recursos.

Para esta muestra se puede mencionar acerca de la magnitud de sus metas lo mismo que se expresó para el universo; sin embargo, frente al cumplimiento, se verificó que uno de los proyectos, “*Renovar el soporte y la garantía de la solución FortiDDoS*” por \$ 1.213.000.000, programado para ejecutarse en el último trimestre de 2021, a la fecha no se ha adelantado.

Indagado el proceso acerca de la formulación de los proyectos del PETI, se pudo verificar que en este documento se incluyen como proyectos solamente aquellos que implican procesos contractuales; que los tiempos descritos son los que corresponden a la ejecución del contrato y el valor es el que se ha determinado mediante estudios, que es suficiente para cubrir dicha obligación. Sin embargo, fruto de esta formulación, no se incluyen en el documento, la cuantificación de los productos, ni las metas asociadas a las brechas o avances que se busca cubrir por este medio.

El PETI se encuentra medido por un único indicador que opera la STRT, pero que no se describe en el documento, y es por medio de la determinación del número de proyectos adelantados (contratados), este indicador no se encuentra registrado en ningún sistema de medición de la gestión como tal y es un control no documentado que ejecuta el proceso para su seguimiento. Esta medición no incluye un componente de oportunidad en el cumplimiento de la programación, por lo que se reduce a señalar el momento en el cual se contrata un nuevo proyecto.

El PETI se encuentra ajustado a los recursos asignados anualmente en el presupuesto liquidado en el decreto anual del Distrito para su primer año de elaboración o ajuste, por lo que su proyección presupuestaria para las vigencias siguientes, es decir, del segundo al cuarto año, son parciales y no cubren las necesidades propias de la gestión institucional en materia de TI. Al respecto la Guía contempla en su numeral “*2.8.4 Proyección de presupuesto área de TI Se debe realizar la planeación de los recursos financieros necesarios para llevar a cabo la implementación del PETI. En todo momento la planeación de los recursos financieros debe estar actualizada y se debe realizar seguimiento a su ejecución mínimo cada mes.*”

Se recomienda que se cuantifique de manera completa el PETI en el periodo para el que se formula, para el caso en comento, el cuatrienio 2021-2024, de manera que se determinen las necesidades de dicho periodo y se estime la totalidad de recursos necesarios para su cumplimiento.

Finalmente, en lo correspondiente al Plan de Comunicaciones del PETI, en la versión 14, no se desarrolló el tema y solamente se registraron las descripciones de los ítems a tener en cuenta para su formulación.

Como hecho posterior al periodo auditado, se verificó que el 16/11/2022, el Comité Institucional de Gestión y Desempeño aprobó la versión 15 del PETI del IDU, pero se encuentra pendiente su publicación hasta

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

tanto se determine el monto definitivo de recursos asignados en el presupuesto del Instituto para la vigencia 2023. Por tal razón, el análisis plasmado en este informe frente al PETI, corresponde a la versión 14, vigente para el alcance temporal de esta auditoría, y no fue posible hacer el ejercicio de comparación con la versión 15, por lo que es necesario que el personal del proceso contraste las recomendaciones realizadas al respecto por el equipo auditor, frente a la versión 15.

Se recomienda que se siga el lineamiento de la Guía G.ES.06 y se realicen las actualizaciones anualmente, sin exceder los doce meses, por cuanto periodos más amplios, como el que se presenta entre la expedición de las versiones 14 (enero de 2021) y 15 (noviembre de 2022), hacen que muchos de los componentes pierdan actualidad durante la vigencia de la versión correspondiente.

Se recomienda revisar las observaciones registradas en este informe y los detalles expresados en las reuniones de auditoría para fortalecer el PETI y presentar una versión mejorada, en lo posible en la número 15, toda vez que, al no haber sido publicada, podría ser revisada nuevamente por el Comité Institucional Gestión y Desempeño para contar, en la vigencia 2023, con un documento actualizado y más alineado a los criterios propuestos en la Guía G.ES.06 del MinTIC.

2. Plan de adquisiciones TI / Plan de contratación TI

Para adelantar este análisis, se tomó una muestra superior al 60 % de lo referido en el PETI “*Tabla 40 Mapa de Ruta de Proyectos Plan anual de adquisiciones*”, correspondiente a las nueve contrataciones de mayor valor y sus dos complementos.

Como se aprecia en la tabla siguiente, estas contrataciones, que aparecen en la tabla 40 del PETI 2021, alcanzan un valor de \$16.887.729.000, equivalente al 60,09 % del valor registrado en dicha tabla para ser incluido en el Plan Anual de Adquisiciones \$ 28.105.599.000 y corresponden tanto a la adquisición de bienes tangibles como intangibles, sin dejar de lado los servicios de mantenimiento, soporte y garantía.

La adquisición de los bienes y servicios referidos en la muestra se programó para la vigencia 2021.

La información contractual fue suministrada por el proceso mediante el diligenciamiento de un cuadro Excel y aportó evidencias como los contratos y las actas de recibo, terminación o liquidación, que correspondieran, según el tipo de contratación.

Tabla N.º 1. Muestra de la contratación 2021

Nº	PROYECTO	VIGENCIA	PLAZO	VALOR (\$)
1	Adquisición y renovación de software por catálogo del Acuerdo Licenciamiento Corporativo (ELA) que soporta la operación y el desarrollo del Sistema de Información Geográfico del Instituto de Desarrollo Urbano - SIGIDU	2021	365	1.490.000.000
2	Contratar los servicios de soporte, mantenimiento y desarrollos sobre el Sistema de Información Valorizamos	2021	365	1.058.729.000
3	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	2021	365	3.330.000.000
4	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	2021	365	231.000.000
5	Contratar los servicios de consultoría para desarrollar la ejecución del segundo ciclo de arquitectura empresarial alineado con el marco de referencia de arquitectura empresarial para la gestión de tecnologías de la información del estado Colombiano	2021	365	1.400.000.000
6	Contratar la segunda fase de la solución de espacio digital de trabajo - Escritorio Remoto Virtualizado (VDI)	2021	120	1.488.000.000

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Nº	PROYECTO	VIGENCIA	PLAZO	VALOR (\$)
7	Ampliar la capacidad de procesamiento, almacenamiento y virtualización a través de una solución de hiperconvergencia	2021	180	2.100.000.000
8	Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano	2021	120	1.642.000.000
9	Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano	2021	120	455.000.000
10	Renovar el soporte y la garantía de la solución FortiDDoS	2021		1.213.000.000
11	Adquisición de licencias nuevas y renovación, soporte, actualización y mantenimiento (SAM) de software especializado para procesos de ingeniería en infraestructura civil y de movilidad del IDU.	2021	60	2.480.000.000
TOTAL				16.887.729.000
% de cobertura del presupuesto de la vigencia (\$ 28,105,599,000)				60,09 %

Fuente: información suministrada por la STRT. Elaboración: equipo auditor.

Tabla N.º 2. Plazos de ejecución

Nº	PROYECTO	PLAZO	Nº CONTRATO	FECHA		PLAZO REAL	FECHA PROGRAMADA EN PETI	BRECHA TIEMPO (DÍAS)	
				INICIO	FIN			2021	2020
1	Adquisición y renovación de software por catálogo del Acuerdo Licenciamiento Corporativo (ELA) que soporta la operación y el desarrollo del Sistema de Información Geográfico del Instituto de Desarrollo Urbano - SIGIDU	365	CCE-63840-2021	15-feb-21	14-feb-22	365	30-ene-21	-16	
2	Contratar los servicios de soporte, mantenimiento y desarrollos sobre el Sistema de Información Valoricemos	365	IDU-1534-2021	6-sep-21	5-sep-22	365	30-abr-21	-129	
3	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	365	CCE-69828-2021	9-jun-21	8-jun-22	365	30-abr-21	-40	
4	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	365	CCE-69828-2021	9-jun-21	8-jun-22	365	30-abr-21		
5	Contratar los servicios de consultoría para desarrollar la ejecución del segundo ciclo de arquitectura empresarial alineado con el marco de referencia de arquitectura empresarial para la gestión de tecnologías de la información del estado Colombiano	365	IDU-1671-2021	18-nov-21	22-jul-22	246	31-may-21	-171	
6	Contratar la segunda fase de la solución de espacio digital de trabajo - Escritorio Remoto Virtualizado (VDI)	120	IDU-1346-2020	26-oct-20	25-feb-21	123	31-may-21	217	217
7	Ampliar la capacidad de procesamiento, almacenamiento y virtualización a través de una solución de hiperconvergencia	180	IDU-1434-2022	7-sep-22	6-abr-23	212	31-may-21	-464	
8	Compra de equipos de tecnología para usuario final	120	CCE-74413-2021	25-ago-21	24-dic-21	122	31-jul-21	-25	

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Nº	PROYECTO	PLAZO	Nº CONTRATO	FECHA		PLAZO REAL	FECHA PROGRAMADA EN PETI	BRECHA TIEMPO (DÍAS)	
				INICIO	FIN			2021	2020
	del Instituto de Desarrollo Urbano								
9	Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano	120	CCE-74413-2021	25-ago-21	24-dic-21	122	31-jul-21		
10	Renovar el soporte y la garantía de la solución FortiDDoS		No realizado				30-sep-21	-426	
11	Adquisición de licencias nuevas y renovación, soporte, actualización y mantenimiento (SAM) de software especializado para procesos de ingeniería en infraestructura civil y de movilidad del IDU.	60	IDU-507-2022 IDU-508-2022 IDU-509-2022 IDU-510-2022 IDU-511-2022 IDU-512-2022 IDU-513-2022	28-feb-22	3-jul-22	126	30-nov-21	-90	
TOTAL								-1.144	217

Fuente: información suministrada por la STRT. Elaboración: equipo auditor.

De acuerdo con la información suministrada por el proceso, como se aprecia en la tabla anterior, se pudo establecer que los procesos contractuales planteados como muestra, no se efectuaron en las fechas contempladas en la programación registrada en el PETI.

Se tiene que, a la fecha de esta auditoría, no se ha realizado la contratación del Ítem 10, “Renovar el soporte y la garantía de la solución FortiDDoS”, acumulando una mora de 425 días, así como la demora en contratar el ítem 7 “Ampliar la capacidad de procesamiento, almacenamiento y virtualización a través de una solución de hiperconvergencia”, que acumuló 464 días para ser cumplida. Lo anterior contrasta con la contratación del ítem 6 “Contratar la segunda fase de la solución de espacio digital de trabajo - Escritorio Remoto Virtualizado (VDI)” que estaba prevista en el PETI para contratarse el 31/05/2021 y se contrató el 26/10/2020.

Así, el aspecto contractual del PETI, acumuló un total de 1.361 días de desfase en relación con las fechas propuestas en la planeación.

Tabla N.º 3. Aspectos presupuestales

Nº	PROYECTO	VALOR (\$)	Nº CONTRATO		% DE AVANCE	VALOR RECURSOS (\$)		
						2021	2020	2022
1	Adquisición y renovación de software por catálogo del Acuerdo Licenciamiento Corporativo (ELA) que soporta la operación y el desarrollo del Sistema de Información Geográfico del Instituto de Desarrollo Urbano – SIGIDU	1.490.000.000	CCE-63840-2021	100%	100%	1.490.000.000		
2	Contratar los servicios de soporte, mantenimiento y desarrollos sobre el Sistema de Información Valoricemos	1.058.729.000	IDU-1534-2021	159,64%	100%	1.690.183.803		
3	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	3.330.000.000	CCE-69828-2021	25,51%	100%	908.276.990		

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Nº	PROYECTO	VALOR (\$)	Nº CONTRATO		% DE AVANCE	VALOR RECURSOS (\$)		
						2021	2020	2022
4	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	231.000.000	CCE-69828-2021		100%			
5	Contratar los servicios de consultoría para desarrollar la ejecución del segundo ciclo de arquitectura empresarial alineado con el marco de referencia de arquitectura empresarial para la gestión de tecnologías de la información del estado Colombiano	1.400.000.000	IDU-1671-2021	159,52%	100%	2.233.217.019		
6	Contratar la segunda fase de la solución de espacio digital de trabajo - Escritorio Remoto Virtualizado (VDI)	1.488.000.000	IDU-1346-2020	42,22%	100%		731.150.000	
7	Ampliar la capacidad de procesamiento, almacenamiento y virtualización a través de una solución de hiperconvergencia	2.100.000.000	IDU-1434-2022	219,44%	29%	4.608.149.653		4.608.149.653
8	Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano	1.642.000.000	CCE-74413-2021	3,47%	100%	72.787.914		
9	Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano	455.000.000	CCE-74413-2021		100%			
10	Renovar el soporte y la garantía de la solución FortiDDoS	1.213.000.000	No realizado	0,00%	0%			
11	Adquisición de licencias nuevas y renovación, soporte, actualización y mantenimiento (SAM) de software especializado para procesos de ingeniería en infraestructura civil y de movilidad del IDU.	2.480.000.000	IDU-507-2022 IDU-508-2022 IDU-509-2022 IDU-510-2022 IDU-511-2022 IDU-512-2022 IDU-513-2022	42,51%	100%	1.054.244.629		1.054.244.629
TOTAL		16.887.729.000				6.394.465.726	731.150.000	5.662.394.282
% de cobertura del presupuesto de la vigencia (\$28,105,599,000)		60,09%			AVANCE EN LA MUESTRA	34,98%	4,33%	33,53%

Fuente: información suministrada por la STRT. Elaboración: equipo auditor.

En cuanto a los valores contratados, con respecto a la muestra, se estableció que, con recursos de la vigencia 2021, se comprometieron el 34,98 % de los recursos establecidos para la contratación analizada, mientras que, con respecto a la misma muestra, se comprometió el 4,33 % con recursos de 2020 y el 33,53 % con recursos de 2022. A la fecha no se han comprometido recursos para la contratación del ítem 10 “Renovar el soporte y garantía de la solución FortiDDoS”.

El ítem 6, “Contratar la segunda fase de la solución de espacio digital de trabajo - Escritorio Remoto Virtualizado (VDI)”, fue adicionado y su meta se vio incrementada, pero solamente alcanzó una ejecución de \$ 731.150.000 (42,22 %) sobre los recursos programados para este ítem (\$ 1.488.000.000).

Los ítems 3 y 4 corresponden al mismo objeto “Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas,” así como los ítems 8 y 9 a “Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano”. La programación de recursos fue de \$ 3.561.000.000 y \$ 2.097.000.000 para

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

cada objeto mencionado; de ellos, se apropiaron \$ 908.276.990 y \$ 72.787.914, respectivamente, correspondientes a 25,51 % y 3,47 %.

Del otro extremo están los ítems 2 “Contratar los servicios de soporte, mantenimiento y desarrollos sobre el Sistema de Información Valoricemos” y 5 “Contratar los servicios de consultoría para desarrollar la ejecución del segundo ciclo de arquitectura empresarial alineado con el marco de referencia de arquitectura empresarial para la gestión de tecnologías de la información del estado Colombiano”, para los cuales se determinó que el valor de la contratación se incrementó al 159,64 % y 159,52 % respectivamente, de los valores planeados.

El ítem 7. “Ampliar la capacidad de procesamiento, almacenamiento y virtualización a través de una solución de hiperconvergencia” se contrató en su totalidad con recursos de la vigencia 2022, y su monto se vio incrementado al 219,44 % del valor programado inicialmente. Éste es el único proceso contractual de la muestra, que a la fecha de esta auditoría se encontraba en ejecución.

Tabla N.º 4. Estado de la contratación y Meta física

Nº	PROYECTO	Nº CONTRATO	% AVANCE	META CONTRATADA	META ADICIONAL	ACTA DE RECIBO
1	Adquisición y renovación de software por catálogo del Acuerdo Licenciamiento Corporativo (ELA) que soporta la operación y el desarrollo del Sistema de Información Geográfico del Instituto de Desarrollo Urbano - SIGIDU	CCE-63840-2021	100%	Adquisición y renovación de software por catálogo		Liquidado
2	Contratar los servicios de soporte, mantenimiento y desarrollos sobre el Sistema de Información Valoricemos	IDU-1534-2021	100%	12 meses soporte y mnto, y 5680 Horas		En proceso de liquidación
3	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	CCE-69828-2021	100%	Servicio de correo electrónico y herramientas colaborativas		Liquidado
4	Contratar los servicios de Plataforma de correo institucional y herramientas colaborativas	CCE-69828-2021	100%			Liquidado
5	Contratar los servicios de consultoría para desarrollar la ejecución del segundo ciclo de arquitectura empresarial alineado con el marco de referencia de arquitectura empresarial para la gestión de tecnologías de la información del estado Colombiano	IDU-1671-2021	100%	5 fases y Cinco productos		En proceso de liquidación
6	Contratar la segunda fase de la solución de espacio digital de trabajo - Escritorio Remoto Virtualizado (VDI)	IDU-1346-2020	100%	100	60	Liquidado
7	Ampliar la capacidad de procesamiento, almacenamiento y virtualización a través de una solución de hiperconvergencia	IDU-1434-2022	29%			En ejecución
8	Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano	CCE-74413-2021	100%			Liquidado
9	Compra de equipos de tecnología para usuario final del Instituto de Desarrollo Urbano	CCE-74413-2021	100%			Liquidado
10	Renovar el soporte y la garantía de la solución FortiDDoS	No realizado	0%			
11	Adquisición de licencias nuevas y renovación, soporte, actualización y mantenimiento (SAM) de software especializado para procesos de ingeniería en infraestructura civil y de movilidad del IDU.	IDU-507-2022 IDU-508-2022 IDU-509-2022 IDU-510-2022 IDU-511-2022 IDU-512-2022 IDU-513-2022	100%			Terminado no requiere acta de liquidación

Fuente: información suministrada por la STRT. **Elaboración:** equipo auditor.

Para los diez primeros ítems, se han adelantado ocho procesos contractuales, de ellos, seis se encuentran terminados o liquidados, uno en proceso de liquidación y uno en ejecución, el ítem 10, como se observa, a la fecha no se ha contratado.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Con respecto a la meta física, a partir del PETI no es posible determinar su magnitud, por cuanto en el documento y en los complementos no se encuentra cuantificada. Los porcentajes de avance presentados en la tabla precedente se registraron según la información suministrada por el proceso.

El ítem 11, se contrató por lotes (7), de acuerdo con lo informado por el proceso, por cuanto el concepto era software especializado. Al revisar la adjudicación, se pudo establecer que seis de las siete contrataciones se adjudicaron a un mismo contratista (COMPUTADORES Y SOLUCIONES CAD DE COLOMBIA S.A.S.), por lo que se recomienda verificar la pertinencia de este tipo de desagregación contractual para los futuros procesos contractuales como los descritos en el ítem 11.

3. Matriz de riesgos institucionales del proceso

A continuación, se presenta el análisis de riesgos de corrupción y de gestión del proceso de Gestión de Tecnologías de Información y Comunicación, el cual pretende orientar para que se evalúe el ajuste o modificación de los componentes de los riesgos, tales como causas, controles, frecuencias, responsables, entre otros, con el fin de aportar a la toma de decisiones del proceso. Para mejor comprensión de este aparte se sugiere consultar el Anexo N.º 1.

La matriz de riesgos institucionales del proceso se compone de seis riesgos identificados por el proceso, dos de ellos son de corrupción y los cuatro restantes son de gestión. Al respecto se realizan las siguientes observaciones, con base en la matriz que se encuentra publicada:

RIESGOS DE CORRUPCIÓN:

- *C.TI.01 Acceso indebido para manipular o adulterar datos almacenados en los servidores de la Entidad, en beneficio propio o de un tercero. (Integridad).*

Las causas identificadas con los números 1 y 2, con base en su redacción, son controles mal aplicados, es decir, no corresponden a la definición de causa. La causa identificada con el número 3, es un evento de riesgo, no una causa.

Frente a las causas raíz: la raíz 1, no desarrolla la manera en la cual puede ser una causa de acceso indebido a los servidores. La raíz número 2 es un ejemplo de la causa 2. Finalmente, la causa raíz 3 corresponde a controles mal aplicados.

Con respecto a los controles, el relacionado con el sistema de autenticación basado en el directorio activo tiene una debilidad en torno a su actualización por cuanto, en algunos aplicativos, no se registran los cambios con la oportunidad que se dan las modificaciones temporales o permanentes del personal de la entidad; en otros casos, al operar de manera simultánea el usuario fijo con el temporal de un funcionario que se encuentra encargado de otra dependencia, se han generado conflictos que inactivan uno de los dos; y también se han detectado casos, particularmente en aplicativos basados en la plataforma Odo, en los cuales un usuario está asociado a una dependencia a la que no pertenece. Se recomienda verificar los aspectos técnicos que están generando estas fallas en el control.

Los encargados enunciados en el control 2, no se encuentran con los roles actualizados.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

El tercer control hace referencia a las autorizaciones de acceso con registro por CHIE: Gestión TIC, sin embargo, hay solicitudes de acceso, a sistemas de información o recursos de TI, tales como ZIPA o CHIE-Planes de Mejoramiento, que no se registran en dicho sistema. Se recomienda actualizar esta otra modalidad de solicitud, por cuanto se está limitando el control a una única forma de registro previo de las autorizaciones, pero hay un registro último que no se menciona y es en la mesa de ayuda (herramienta ARANDA), donde finalmente se debe dejar traza de todas las solicitudes.

El cuarto control deja como responsabilidad de los jefes de cada dependencia o líderes de proceso el reportar bimestralmente los usuarios inactivos, sean temporales o definitivos, luego de una solicitud de la STRT. No hace referencia o incluye los casos de usuarios en situaciones administrativas (licencias, suspensión de contrato, entre otras) durante los periodos no solicitados por la STRT.

Adicionalmente, se observó que hay una incongruencia con lo indicado en el instructivo IN-TI-16 “*Revisión de los Derechos de Acceso a los Recursos de TI*”, dado que en éste refiere que la verificación se hace una vez al año, pues indica que “*Durante cada vigencia, la STRT realizará una verificación de usuarios y generará un informe consignando las cuentas de usuarios registrados en el servicio del Directorio Activo*”². Se recomienda efectuar el ajuste que corresponda, ya sea en el Instructivo o en la matriz de riesgos de corrupción, para asegurar la consistencia documental.

Se verificó que los certificados SSL se encuentran activados en los sitios web de la entidad y operan de acuerdo con lo establecido.

Como se manifestó en las reuniones, debe realizarse una revisión, diferenciación y actualización de la documentación y las evidencias registradas, también de los responsables.

Con respecto a los tratamientos descritos en la matriz, se deben diferenciar de los controles habituales del proceso, por cuanto están registrados como tratamiento, con algunas diferencias de redacción, los mismos controles que hacen parte del procedimiento de gestión habitual.

- *C.TI.02 Revelar información de carácter confidencial a terceros que se vean beneficiados por la oportunidad de la misma.*

Las tres causas enunciadas no demuestran una conducta con intención, por lo que no encuadran en una causa para un riesgo de corrupción.

Las causas raíz son versiones alternativas de las causas descritas.

El control 1 hace referencia a controles del proceso de gestión documental. En la entrevista, el personal del proceso mencionó como información confidencial la correspondiente a los procesos contractuales, pero no hay referencia a documentos de carácter técnico del proceso, por lo que no se aprecia una adecuada concordancia entre el alcance del riesgo y las causas.

El control 2, se refiere a las medidas generales de seguridad de la información, pero al no definirse los documentos clasificados o reservados del proceso, no es clara su utilidad como control para este riesgo.

² Ver numeral “5.1 Revisión de los accesos a la red institucional y a los sistemas de información según el perfil de usuario” del instructivo IN-TI-16.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

El control 3, también hace parte de las medidas generales de seguridad de la información, pero al no definirse los documentos clasificados o reservados del proceso, tampoco es clara su utilidad como control para este riesgo.

Para los riesgos de corrupción, se recomienda que, en la próxima actualización o en una extraordinaria, sean revisados y se verifique cada uno de los elementos que los describen, teniendo en cuenta las observaciones de este informe, verificando y precisando los aspectos presentes y se establezca si hay necesidad de ampliar algunos aspectos como los mencionados anteriormente.

RIESGOS DE GESTIÓN

- *G.TI.01 Inadecuada definición de los requerimientos del software a desarrollar.*

Las causas 1 y la afirmación final de la 2 se encuentran relacionadas en cuanto a que son temas documentales, con respecto a la 3, se aprecia una relación entre la 1 y ella por cuanto las metodologías incluyen el empleo de buenas prácticas.

Con respecto a las causas raíz: de la raíz 1, los entregables hacen parte de la metodología, por lo que hace parte de la causa raíz 3 y la causa raíz 3 evidencia el origen de lo expresado en la causa 3. Ahora bien, lo expresado en la causa raíz 2 no tiene relación con la causa de falta de compromiso y responsabilidad, son dos circunstancias independientes de lo que se considera causa raíz.

Se considera importante determinar si se cuenta o no con una metodología de definición de los requerimientos del software a desarrollar y si ella emplea, alienta el empleo o no de las buenas prácticas para de esta manera poder evaluar la pertinencia de los controles que se mencionan.

Con respecto al control 1, se recomienda determinar claramente los cargos y roles de quienes lo ejecutan y ajustarlo frente a la metodología que se esté aplicando, de manera que se constituya en un elemento de control efectivo y queden las evidencias correspondientes.

El control 2 debe dejarse documentado, bien sea mediante la suscripción del documento o algún otro elemento que permita la verificación de su cumplimiento.

El control 3 es el mismo control 1.

El tratamiento a que se hace referencia en la matriz es la descripción del procedimiento que se está efectuando, por lo que no corresponde a un tratamiento, sino a la descripción de los controles habituales de la gestión.

- *G.TI.02 Insuficiente asignación de recursos para el cumplimiento de los objetivos o actividades requeridas por el proceso.*

La causa 1 es una falla o desviación que podría darse en la ejecución del control planteado para la misma, no es una causa. La causa 2 corresponde, realmente, a una consecuencia y la causa 3 es la misma descripción del riesgo.

Con respecto a las causas raíz, la primera no tiene relación con el riesgo, mientras que la segunda y tercera son la misma causa raíz, pero describen dos elementos diferentes.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

El control 1 se encuentra sistematizado en torno a las herramientas tecnológicas que se verifican, pero no fue posible determinar que se lleve a cabo con la frecuencia establecida, por cuanto no se dejan registros de su ejecución periódica.

El control 2 en su definición es un tratamiento: puede tratarse como preventivo, al llegar a un punto de control o como remedial al superar las capacidades necesarias. Su redacción también presenta vacíos en torno al criterio que rige la acción esperada de los responsables frente al control y lo presenta como potestativo (puede o no efectuarse) y no como imperativo (debe hacerse).

El control 3 también corresponde a un tratamiento de contingencias. No se evidencia claridad en torno a las condiciones de funciones y compromisos contractuales de quienes pudieran ser incluidos en el plan de atención de la situación. La redacción da pie a suponer que no se garantiza que el servicio sea prestado por personal idóneo (legal y/o técnicamente) y que podría presentarse extralimitación de funciones o la prestación de un servicio por un contratista que no sea competente legal o técnicamente.

El control 4 no corresponde a un control puesto que es el procedimiento de gestión de recursos sobre el cual se deben determinar los controles para que se asignen de manera pertinente y suficiente los recursos necesarios por el proceso.

Los tratamientos descritos en el formato son, realmente, acciones propias de los procedimientos ya establecidos y no tiene capacidad para alterar los resultados de la materialización del riesgo.

- *G.TI.03 Inadecuada gestión de la Infraestructura de TI.*

En concepto del equipo auditor, la inadecuada gestión de la Infraestructura de TI no es un riesgo, es una falla de la operación y como tal no corresponde a una situación que se encuentre contenida en la definición de riesgo.

La causa 1 es una falla del servicio que se puede catalogar como una situación particular de la falla registrada como riesgo.

La causa 2 es una falla en la operación de un control (copias de seguridad).

La causa 3 Es una consecuencia de la inadecuada gestión de los recursos tecnológicos.

Con respecto a las causas raíz, es importante manifestar que la 1 denota la falta de controles, la 2 es una omisión en la operación de los controles y la 3 no se encuentra redactada como causa, antes bien pareciera un control.

En el control 1 no se identifica qué se entiende por servicios básicos redundantes o cuáles son éstos, además se hace referencia a servicios contratados, pero se registra como evidencia el balanceador de cargas y las UPS, elementos que no son redundancia de un servicio contratado.

Respecto del control 2, no se identifica con claridad cómo se relaciona con la gestión de infraestructura. Es un control manual, se recomienda sistematizar el registro de las solicitudes de copias de seguridad para identificar la completitud de su aplicación.

FORMATO		
INFORME DE AUDITORIA		
CÓDIGO	PROCESO	VERSIÓN
FO-EC-111	EVALUACIÓN Y CONTROL	1.0



El control 3 responde a un criterio individual de quien lo opera, y corresponde a una verificación de inventario de infraestructura que no necesariamente permite determinar el riesgo tecnológico de obsolescencia.

La redacción del control 4 expresa que se puede o no llevar a cabo el control de manera anual y no tiene consecuencias.

El control 5 que administra los parches de seguridad, es automático y tiene la opción manual. No se encuentra relación de su propósito con el riesgo descrito.

El control 6 hace referencia a las restricciones automáticas de instalación de software, pero su redacción permite identificar que el proceso conoce de sus limitaciones y que su grado de efectividad no es el deseado, por lo que enseguida plantea como respaldo un tratamiento de corrección manual.

Se enuncia como control 7 “*Incluir Control mantenimiento Correctivo*”, pero no se describe. Es importante mencionar que en la auditoría MIPG SIG 2022 se identificó que en la versión de la matriz de riesgos institucional de enero de 2022 figuraba el control “*7 El líder (sic) del equipo de infraestructura en caso de requerirse, solicita mantenimiento correctivo, mediante un contrato apropiado. Como evidencia se tienen los contratos de mantenimiento*”, pero fue eliminado para la versión publicada en el seguimiento efectuado con corte 30/04/2022, y reemplazado por el texto ya mencionado.

Esta situación dio lugar a la recomendación de efectuar las correcciones para complementar la información de descripción de dicho control, así como realizar las acciones respectivas ante la OAP para que se vean reflejadas en la matriz publicada en la Intranet, que se reitera en el presente informe.

Los tratamientos registrados no pueden identificarse como tales.

- *G.TI.14 Lentitud en la respuesta de los servicios de red interna o externa.*

La manera en como está redactado el riesgo describe una situación que correspondería a una falla de la operación y como tal no corresponde a una situación que se encuentre contenida en la definición de riesgo.

La causa 1 es un tipo de fallo del control. La causa 2 es una mala operación de los controles. La causa 3, como está descrita, no tiene relación de causalidad con el riesgo, toda vez que no se identifica el sujeto que puede llegar a generarlo.

Con respecto a las causas raíz: la 1 es un fallo en la definición del control, al igual que la 2, la 3 no identifica al sujeto y es una falla de control.

El control 1 salvaguarda los sistemas de descargas no autorizadas, pero no tiene relación con el tema de velocidad en la respuesta de servicios de red.

El control 2 salvaguarda los sistemas de intrusos, pero no tiene relación con el tema de velocidad en la respuesta de servicios de red.

El control 3 aporta con la divulgación de las normas de uso de los recursos de red, pero debido a las dificultades para definir el riesgo y sus causas no es clara la relación del riesgo con el control propuesto.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

El registro de tráfico en la red no es un tratamiento de riesgo, por cuanto un registro no puede mitigar, reparar o prevenir un riesgo o sus causas.

Para los riesgos de Gestión, se recomienda que, en la próxima actualización o en una extraordinaria, sean revisados cada uno de los elementos que los describen, teniendo en cuenta las observaciones de este informe y se establezca si hay necesidad de ampliar algunos aspectos con base en lo registrado en este informe.

Se considera importante que se informe de este análisis a la Oficina Asesora de Planeación – OAP para que, en su papel de administrador del riesgo a nivel institucional, se determine la pertinencia de realizar ajustes en los lineamientos frente a la definición de algunas de las variables relacionadas en la matriz de riesgos, como la definición del riesgo, causas, controles, responsables, entre otras.

Actividad crítica 2. Administración de Infraestructura de T.I.

De acuerdo con la caracterización del proceso de Gestión de Tecnologías de Información y Comunicación, esta actividad crítica se relaciona con diversos aspectos del proceso, a saber:

“Controlar el ciclo de instalación, configuración, aseguramiento, funcionamiento, capacidad de recursos y retiro de servidores de procesamiento y almacenamiento, para la atención de los servicios de tecnología desplegados y en proceso de implementación, que requiere el Instituto para el cumplimiento de sus objetivos.

Gestionar la generación y restauración de copias de respaldo.

Velar por el adecuado control de ingreso de personal al centro de cómputo y a la zona de alistamiento; gestionar el suministro de servicios de aire acondicionado del centro de cómputo. Efectuar el monitoreo de las condiciones ambientales, de los elementos de prevención y extinción de fuego y de alerta de los elementos contenidos en el centro de cómputo.

Gestionar la red de datos de la Entidad, contemplando las medidas de seguridad y control necesarias para mantener la integridad, confidencialidad y disponibilidad de la información del Instituto.

Administrar el plan de capacidad y disponibilidad de los recursos de tecnología, incluyendo más no limitándose a almacenamiento, procesamiento y redes de datos, necesarios para la adecuada prestación de los servicios de TI”.

Para la revisión en la presente auditoría se seleccionaron los productos o salidas “2. Administración de Infraestructura de T.I”. Productos “2. Gestión de capacidad”, “3. Copia de respaldo ordinaria”, “4. Copia de respaldo por demanda” y “5. Información restaurada”. A continuación, se presenta la información correspondiente frente a cada uno de estos productos:

1. Gestión de capacidad

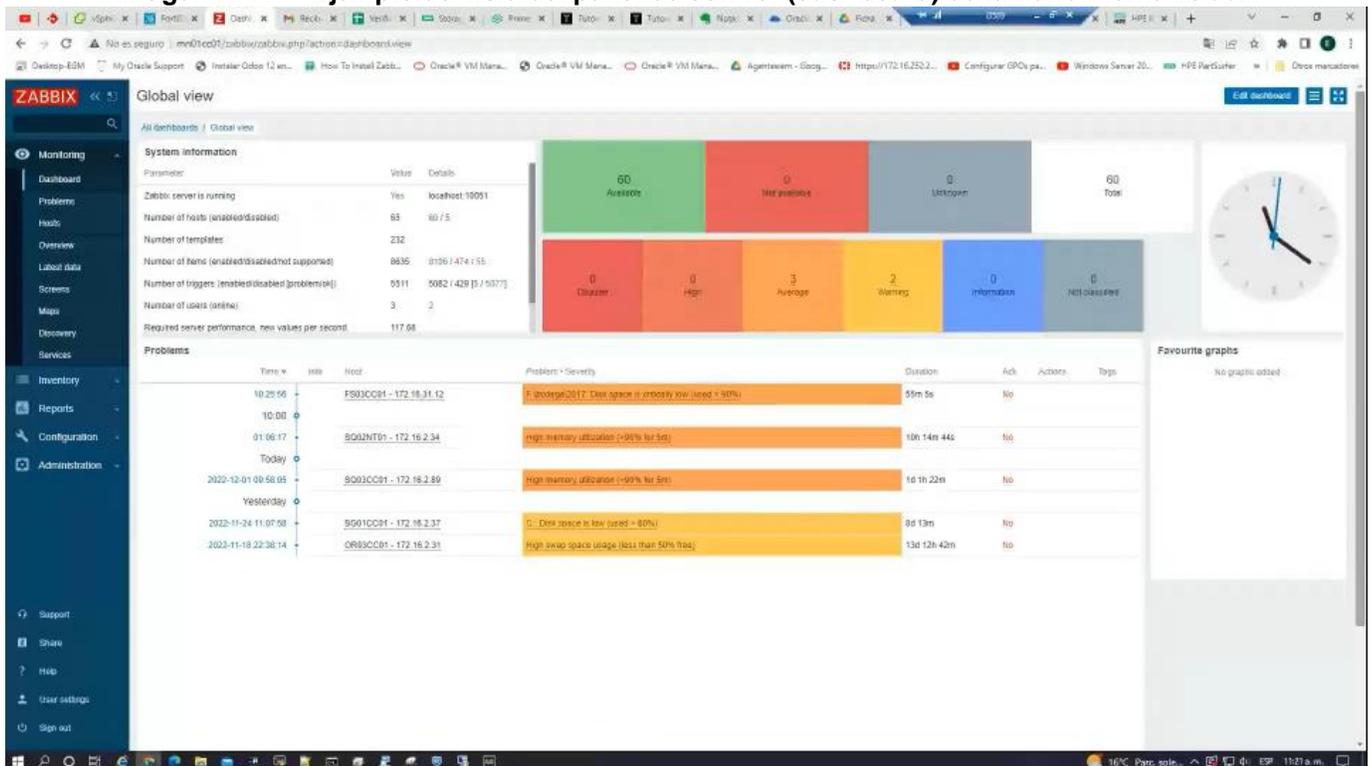
De acuerdo con lo informado por personal de la STRT, la gestión de la capacidad de Tecnologías de Información (TI) se está realizando de dos formas: diariamente y a través de un histórico con el diligenciamiento del formato FO-TI-30.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Diariamente se está realizando mediante la utilización de la herramienta Zabbix³ para revisar disponibilidad y capacidad (salud de los equipos). Antes utilizaban la herramienta Nagios, también de software libre. De acuerdo con lo informado en entrevista de auditoría sobre el tema, la decisión de reemplazo fue tomada dadas las mejoras en la administración y presentación que provee la herramienta actual, entre estas la obtención de reportes, dado que en Nagios los datos se almacenan en texto plano, pero que en Zabbix se pueden almacenar en formatos de bases de datos.

La STRT está haciendo uso de la herramienta desde, aproximadamente, febrero de 2022, y las funcionalidades básicas de monitoreo de infraestructura ya están operando. El personal entrevistado informó que continúan efectuando gestiones para implementar funcionalidades adicionales de la herramienta que puedan contribuir al monitoreo de otros elementos como páginas web, bases de datos o accesos remotos, entre otras, con el fin de obtener el mayor provecho de la misma.

Imagen N.º 1. Ejemplo de vista del panel de control (dashboard) de la herramienta Zabbix



Fuente: Pantallazo obtenido de la entrevista de auditoría del 02/12/2022.

Esta herramienta permite ver la disponibilidad de elementos, si están activos o no, genera alertas que pueden referirse a diferentes aspectos como consumo de CPU, uso de espacio en disco duro, estado de la memoria, entre otros, respecto de una línea base o umbral establecido (que puede contemplar factores de tiempo y recurso). Las alertas se analizan con los líderes o responsables de los recursos y se evalúan con el fin de determinar si hay problemas para atender y/o si hay lugar a efectuar cambios como aumento de recursos.

³ Zabbix es un software libre de monitoreo del estado de diversos servicios e infraestructura de TI.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

De acuerdo con lista suministrada por la STRT, al 02/12/2022 se encontraban en monitoreo 51 servidores. A manera de ejemplo, la imagen siguiente muestra cómo, en Zabbix y de manera gráfica, se puede observar el consumo o uso de recursos de CPU en uno de los servidores monitoreado y la configuración de la línea base con el *trigger* o condición que generaría la alerta (para el ejemplo: uso privilegiado de CPU mayor al 30 % por 5 minutos o más).

Imagen N.º 2. Ejemplo de vista gráfica de alertas en la herramienta Zabbix



Fuente: Pantallazo obtenido de la entrevista de auditoría del 02/12/2022.

El personal de la STRT mencionó dos ejemplos en los cuales el monitoreo diario de las alertas de sobrecarga de unos servidores que soportan los sistemas SIGIDU (Sistema de Información Geográfica del IDU) y Repositorio de Documentación Relacionada con Proyectos Misionales (el cual se encuentra montado en Dspace) les permitieron anticiparse a una posible caída de los servicios relacionados derivada de la insuficiencia de recursos que requerían tales aplicativos.

La otra forma empleada para la gestión de la capacidad es la utilización del formato FO-TI-30 "Control de la Capacidad de los Recursos de TI". Para el diligenciamiento se desarrolló un *script* o programa que genera un archivo de datos que incluye uso de CPU, memoria y disco (espacio libre) de los distintos servidores, tomando la información del sistema de administración o gestión de eventos y de información de seguridad SIEM (Security Information and Event Management). Esto se haría semanalmente.

Al momento de la auditoría se evidenció que el formato utilizado, si bien está identificado con el mismo código (FO-TI-30) y versión (1.0) del publicado en el mapa de procesos de la entidad y en el sistema SUE: Información Documentada, no corresponde con la estructura de éste último. De acuerdo con la explicación de la STRT, lo presentado en la entrevista es un piloto que pretende automatizar la forma de recolección,

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

registro y presentación de datos en el FO-TI-30, de manera que se incremente la frecuencia de recolección y la posibilidad de mantener una cantidad mayor de datos históricos en un mismo archivo. Se recomienda entonces asegurar que, una vez se apruebe este piloto, en el sistema de información documentada SUE se efectúen las gestiones que correspondan para el ajuste y actualización de versión del FO-TI-30, dado que el formato hace parte de los documentos del Sistema Integrado de Gestión MIPG-SIG.

Imagen N.º 3. Ejemplo de cómo se ve el resultado del piloto de automatización del formato FO-TI-30

FORMATO																																																																																																																													
CONTROL DE LA CAPACIDAD DE LOS RECURSOS DE TI																																																																																																																													
CÓDIGO		PROCESO				VERSIÓN		Actualizar																																																																																																																					
FO-TI-30		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN				1.0																																																																																																																							
Id.	Nombre Elemento	SO	IP	Cap. Nominal	Cap. Real	Id.	Nombre Elemento	SO	IP	Cap. Nominal	Cap. Real	Id.																																																																																																																	
1	GI06CC01	Microsoft Windows Server 2012 R2	172.16.31.102			2	SQ02NT01	Microsoft Windows Server 2008 R2	172.16.2.34			3																																																																																																																	
Función del Elemento:						Función del Elemento:																																																																																																																							
Device: GI06CC01						Device: SQ02NT01																																																																																																																							
<table border="1"> <thead> <tr> <th>FechaA</th> <th>CPUUtil</th> <th>MemUtil</th> <th>DiskFree</th> <th colspan="2">Anotación</th> </tr> </thead> <tbody> <tr><td>1925784664</td><td>11.86</td><td>79.97</td><td>39105</td><td colspan="2"></td></tr> <tr><td>19258692200</td><td>11.33</td><td>79.91</td><td>38961</td><td colspan="2"></td></tr> <tr><td>19265232160</td><td>8.83</td><td>84.39</td><td>36644</td><td colspan="2"></td></tr> <tr><td>19265232685</td><td>9.28</td><td>84.39</td><td>36644</td><td colspan="2"></td></tr> <tr><td>1926546350</td><td>9.28</td><td>84.4</td><td>36643</td><td colspan="2"></td></tr> <tr><td>19268067654</td><td>13.9</td><td>84.07</td><td>35384</td><td colspan="2"></td></tr> <tr><td>19275067807</td><td>5.77</td><td>80.8</td><td>33769</td><td colspan="2"></td></tr> <tr><td>19303067618</td><td>9.77</td><td>38.63</td><td>42232</td><td colspan="2"></td></tr> <tr><td>19310067683</td><td>9.68</td><td>41.73</td><td>41409</td><td colspan="2"></td></tr> <tr><td>19317067618</td><td>11</td><td>42.2</td><td>40522</td><td colspan="2"></td></tr> </tbody> </table>						FechaA	CPUUtil	MemUtil	DiskFree	Anotación		1925784664	11.86	79.97	39105			19258692200	11.33	79.91	38961			19265232160	8.83	84.39	36644			19265232685	9.28	84.39	36644			1926546350	9.28	84.4	36643			19268067654	13.9	84.07	35384			19275067807	5.77	80.8	33769			19303067618	9.77	38.63	42232			19310067683	9.68	41.73	41409			19317067618	11	42.2	40522			<table border="1"> <thead> <tr> <th>FechaA</th> <th>CPUUtil</th> <th>MemUtil</th> <th>DiskFree</th> <th colspan="2">Anotación</th> </tr> </thead> <tbody> <tr><td>1925807679</td><td>4.31</td><td>91.86</td><td>10674</td><td colspan="2"></td></tr> <tr><td>19265232160</td><td>3.79</td><td>94.45</td><td>10037</td><td colspan="2"></td></tr> <tr><td>19265232685</td><td>3.79</td><td>94.45</td><td>10037</td><td colspan="2"></td></tr> <tr><td>19265233382</td><td>3.52</td><td>94.46</td><td>10037</td><td colspan="2"></td></tr> <tr><td>19275067807</td><td>69.41</td><td>92.05</td><td>9408</td><td colspan="2"></td></tr> <tr><td>19282067716</td><td>67.64</td><td>91.06</td><td>36859</td><td colspan="2"></td></tr> <tr><td>19324067702</td><td>67.54</td><td>91.77</td><td>35507</td><td colspan="2"></td></tr> </tbody> </table>						FechaA	CPUUtil	MemUtil	DiskFree	Anotación		1925807679	4.31	91.86	10674			19265232160	3.79	94.45	10037			19265232685	3.79	94.45	10037			19265233382	3.52	94.46	10037			19275067807	69.41	92.05	9408			19282067716	67.64	91.06	36859			19324067702	67.54	91.77	35507		
FechaA	CPUUtil	MemUtil	DiskFree	Anotación																																																																																																																									
1925784664	11.86	79.97	39105																																																																																																																										
19258692200	11.33	79.91	38961																																																																																																																										
19265232160	8.83	84.39	36644																																																																																																																										
19265232685	9.28	84.39	36644																																																																																																																										
1926546350	9.28	84.4	36643																																																																																																																										
19268067654	13.9	84.07	35384																																																																																																																										
19275067807	5.77	80.8	33769																																																																																																																										
19303067618	9.77	38.63	42232																																																																																																																										
19310067683	9.68	41.73	41409																																																																																																																										
19317067618	11	42.2	40522																																																																																																																										
FechaA	CPUUtil	MemUtil	DiskFree	Anotación																																																																																																																									
1925807679	4.31	91.86	10674																																																																																																																										
19265232160	3.79	94.45	10037																																																																																																																										
19265232685	3.79	94.45	10037																																																																																																																										
19265233382	3.52	94.46	10037																																																																																																																										
19275067807	69.41	92.05	9408																																																																																																																										
19282067716	67.64	91.06	36859																																																																																																																										
19324067702	67.54	91.77	35507																																																																																																																										

Fuente: Recorte del archivo "3. FOTI30_Automatizado.xlsm" suministrado por la STRT. Elaboración: Equipo auditor.

Se hace notar al proceso que, en el archivo piloto presentado, la información registrada en el campo "FechaA" no corresponde a una fecha sino a un valor numérico, lo cual estaría afectando la integridad de la información, pues no se identifica con claridad cuándo se hicieron las mediciones de capacidad. Según lo manifestado por el líder del grupo de infraestructura al momento de la reunión de auditoría, hay elementos que tienen 12 mediciones, lo cual correspondería a 12 semanas, es decir, desde mediados o finales de septiembre de 2022, aproximadamente. Pero, como se observa en la imagen, no es posible identificar tales fechas. Además, hay elementos que no tienen la misma cantidad de mediciones (algunos tienen 10, otros 7 y uno tiene 4). Por tanto, se recomienda asegurar que los datos registrados en el FO-TI-30 sean legibles y obedezcan a estándares o patrones reconocibles para quienes hagan uso del mismo, resguardando la integridad de su contenido.

Es de mencionar que en la revisión efectuada el 03/01/2022 para verificar el cumplimiento de la acción de mejoramiento 2523 "Diligenciar el formato FO-TI-30 de manera automatizada, mediante la creación de un componente tecnológico, que tome la información de capacidad del SIEM", cuya fecha de vencimiento fue el 31/12/2021, se había evidenciado la automatización del formato, razón por la cual se dio por cumplida. La presentación de la información con esa automatización inicial era similar a la estructura del FO-TI-30 vigente (elementos de análisis en filas) y se veía como lo muestra la siguiente imagen:

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Imagen N.º 4. Soporte presentado por la STRT para evidenciar cumplimiento de la acción de mejora 2523

Id.	Nombre Elemento	Tipo	Unidad	Cap. Nominal	Cap. Real	Umbral	Fecha registro	Observaciones
FORMATO								
CONTROL DE LA CAPACIDAD DE LOS RECURSOS DE TI								
PROCESO								
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN						VERSIÓN	Actualizar	
						1,0		
								
407	01	SS04CC01	Microsoft Windows Server 2019	Megabytes	750.000	750.000	75.000	09/nov/2021
408	Función del Elemento: Servidor de almacenamiento (carpetas compartidas)							
409	Device SS04CC01							
410	FechaA CPUUtil MemUtil DiskFree							
411	23/11/2021 22:44 13,83 57,48 18658							
412	23/11/2021 22:49 12,35 57,47 18657							
413	24/11/2021 0:18 15,26 57,53 18660							
414	Anotación							
415								
416								
424	02	SS05CC01	Microsoft Windows Server 2019	Megabytes	300.000	300.000	45.000	09/nov/2021
425	Función del Elemento: Servidor de almacenamiento (carpetas compartidas)							
426	Device SS05CC01							
427	FechaA CPUUtil MemUtil DiskFree							
428	23/11/2021 22:44 0,84 75,39 82901							
429	23/11/2021 22:49 0,89 75,3 82901							
430	24/11/2021 0:18 0,88 75,46 82885							
431	Anotación							
432								
472	03	CD21CC01	Microsoft Windows Server 2019	Megabytes	200.000	200.000	20.000	09/nov/2021
473	Función del Elemento: Controlador de dominio							
474	Device CD21CC01							
475	FechaA CPUUtil MemUtil DiskFree							
476	15/12/2021 19:57 5,94 35,49 7833							
477	15/12/2021 19:56 5,94 35,49 7833							
478	Anotación							

Fuente: CHIE: Plan Mejoramiento Institucional. Soporte registrado por la STRT, acción de mejora 2523.

Comparando las dos imágenes previas, se evidencia que se pretende cambiar la presentación de la información para que los elementos a los cuales se les toman los datos de capacidad queden en columnas y los datos en sí mismos queden registrados en filas, donde cada fila corresponde a una fecha en la que se hizo medición. Esto acorde con la idea de aumentar la frecuencia de medición (pasaría de trimestral a semanal), para tener información más actualizada y de mejorar la presentación para más facilidad de mantenimiento de información histórica. Es decir, con el piloto mencionado se estaría mejorando la automatización ya efectuada.

Respecto de la frecuencia de medición de la capacidad, es esencial citar que dentro de la documentación del proceso está el procedimiento PR-TI-16 "Gestión de la Capacidad", versión 3, del 2020/07/19. En la política operacional de este documento se indica que "Se debe (sic) revisar y actualizar los valores de capacidad de cada uno de los elementos o activos de información más relevantes de los servicios prestados cada tres meses". Igualmente, en la matriz de riesgos, para el riesgo de gestión del proceso G-TI-02 "Insuficiente asignación de recursos para el cumplimiento de los objetivos o actividades requeridas por el proceso" se encuentra establecido el control 1 que indica "Los operadores de DataCenter, trimestralmente realizan la verificación (sic) y monitoreo de la capacidad de procesamiento, almacenamiento centralizado (SAN - NAS) y redes de datos, mediante herramientas de monitorización. En caso de verificar que los recursos están (sic) dentro los umbrales mínimos, (sic) informan al Subdirector Técnico (sic) de Recursos Tecnológicos (sic) para tomar las medidas correspondientes. Como evidencia se dejan los registros en el formato FO-TI-30". (Subrayados fuera del texto original).

Adicionalmente, el procedimiento PR-TI-16, en su numeral 1.6.15. "3 meses", señala "Al inicio de cada ciclo mensual (sic) (antes de los cinco {5} primeros días hábiles) se deberá realizar la siguiente actividad"⁴. Las actividades siguientes son la 1.6.16. "Realizar mediciones periódicas", que señala "En esta actividad, puntualmente se deben revisar uno a uno los elementos o activos de información consignados en el formato de

⁴ Se observa una incongruencia entre el nombre del numeral 1.6.15 "3 meses" y la descripción que indica "[...] cada ciclo mensual [...]". Para efectos de esta auditoría y de acuerdo con lo comentado en la entrevista, se supone sería ciclo trimestral.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Control de la Capacidad de Recursos de TI, en las herramientas de monitoreo correspondientes, con el fin primordial de tomar datos referentes a la capacidad usada en el último periodo de actividad”, y la 1.6.17. “Registrar valores medidos”, en la que se establece que “Los datos identificados en la actividad anterior, se deben consignar el formato de control de la capacidad de los recursos de TI, teniendo en cuenta de diligenciar adecuadamente la fecha de medición, el valor de la capacidad usada y las notas que sean pertinentes. [...]”.

Por tal razón, se solicitó la evidencia de los valores de capacidad registrados durante 2022 en el FO-TI-30. La STRT no pudo ubicar los formatos en el momento de la reunión, aun cuando se evidenció un recurso exclusivo para el registro de la información del piloto. Se recomienda asegurar que esta información, ya sea registrada de forma manual o automatizada, y otra que sea relevante para la gestión de la capacidad esté almacenada y organizada de tal forma que sea de fácil acceso para aquellos que la requieran y en el momento que se necesite, cumpliendo, naturalmente, con los criterios de confidencialidad e integridad.

Ahora bien, en los archivos remitidos están registradas mediciones efectuadas los días 21/01/2022, 10/05/2022, 24/07/2022, y 27/10/2022 a 6 servidores de almacenamiento (de carpetas o recursos compartidos) identificados como SS02CC01, SS03CC01, SS04CC01, SS05CC01, HPE-3PAR-7200 y HPE-PRIMERA. Como se observa, hubo mediciones en los 4 trimestres de 2022, mas no cada tres meses como lo indican la política operacional del procedimiento y el control mencionado. Los retrasos en las mediciones se refieren en la tabla siguiente:

Tabla N.º 5. Retrasos en las mediciones de gestión de la capacidad en 2022

Trimestre	Fechas en las que debió realizarse la toma de datos de capacidad	Fecha de toma Datos de capacidad	Retraso en la medición (En días hábiles) (*)
1: enero a marzo	Entre el 3 y el 7 de enero de 2022 inclusive	21/01/2022	9
2: abril a junio	Entre el 1 y el 7 de abril de 2022 inclusive	10/05/2022	21
3: julio a septiembre	Entre el 1 y el 8 de julio de 2022 inclusive	24/07/2022	10 (**)
4: octubre a diciembre	Entre el 3 y el 7 de octubre de 2022 inclusive	27/10/2022	13

Fuente: archivos de formato FO-TI-30 diligenciados, suministrados por la STRT. **Elaboración:** equipo auditor.

(*) Contados a partir del último día de las fechas en las que debió realizarse la toma de datos de capacidad.

(**) El 24/07/2022 fue un domingo (día no hábil), por tanto, se contó hasta el lunes 25/10/2022.

La vista de uno de los archivos mencionados de gestión de la capacidad, remitidos por la STRT, se muestra en la imagen N.º 5, en la siguiente página.

Comparando la imagen N.º 5 con la imagen N.º 4 se puede observar que, si bien hubo medición en 2022, no se hizo con la herramienta automatizada generada para demostrar el cumplimiento de la acción de mejora 2523. Es decir, a pesar de que la herramienta se generó antes del 31/12/2021.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Imagen N.º 5. Vista del FO-TI-30 diligenciado para los primeros trimestres de 2022

FORMATO								
CONTROL DE LA CAPACIDAD DE LOS RECURSOS DE TI								
CÓDIGO	PROCESO						VERSIÓN	
FO-TI-30	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN						1,0	
Id.	Nombre Elemento	Tipo	Unidad	Cap. Nominal	Cap. Real	Umbral	Fecha registro	Observaciones
	SS02CC01	Almacenamiento	(GB) - Gigabytes	5.600	4.480	3.584	21/01/2022	El storage no permite crecimiento en su capacidad nominal
Función del Elemento: Servidor de almacenamiento, recursos compartidos institucional.				Mediciones				
				Fec. Medición	Cap. Usada	Cap. Disponible	Anotación	
				21/01/2022	3.963	517	La capacidad de almacenamiento utilizada está por encima del umbral	
				10/05/2022	4.003	477		
				24/07/2022	4.068	412		
Id.	Nombre Elemento	Tipo	Unidad	Cap. Nominal	Cap. Real	Umbral	Fecha registro	Observaciones
	SS03CC01	Almacenamiento	(GB) - Gigabytes	5.600	4.480	3.584	21/01/2022	El storage no permite crecimiento en su capacidad nominal
Función del Elemento: Servidor de almacenamiento, recursos compartidos institucional.				Mediciones				
				Fec. Medición	Cap. Usada	Cap. Disponible	Anotación	
				21/01/2022	3.963	517	La capacidad de almacenamiento utilizada está por encima del umbral	
				10/05/2022	4.016	464		
				24/07/2022	4.201	279		
Id.	Nombre Elemento	Tipo	Unidad	Cap. Nominal	Cap. Real	Umbral	Fecha registro	Observaciones
	SS04CC01	Almacenamiento	(GB) - Gigabytes	5.600	4.480	3.584	21/01/2022	El storage no permite crecimiento

Fuente: Recorte del archivo "2. FOTI30_CONTROL_DE_CAPACIDAD_DE_LOS_RECURSOS_DE_TI_V_1.0_AEC.xlsx", suministrado por la STRT. **Elaboración:** Equipo auditor.

Por otra parte, se indagó acerca de si se medía la capacidad a todos los recursos de TI y respecto de cuáles son los criterios para determinar a qué recursos es importante o fundamental hacerle tal medición. La respuesta fue que no se mide capacidad a todos los recursos, sino a aquellos considerados relevantes con base en criterios de funcionalidad (para qué se utilizan), el nivel de utilización del sistema que soportan y/o los elementos que formen parte de la continuidad del negocio acorde con lo identificado en el Análisis de Impacto al Negocio (BIA, por sus siglas en inglés⁵). Sin embargo, tales criterios no se encuentran relacionados en ninguno de los documentos del proceso, por lo cual se recomienda documentarlos.

Adicionalmente, con base en los anterior, serían relevantes servidores de impresión o servidores de bases de datos y/o que soporten sistemas como el SIGIDU, Kactus, Stone, entre otros (algunos de ellos identificados con iniciales como SQ, OR, GI, SI, etc.), pero en la información remitida de las mediciones de cada trimestre no se encontraron relacionados otros recursos, adicionales a los servidores de almacenamiento ya mencionados.

Respecto del análisis de obsolescencia de infraestructura tecnológica, tema que también tiene que ver con gestión de la capacidad, se identificó que está planteado, en el riesgo de gestión del proceso G.TI.03 "Inadecuada gestión de la Infraestructura de TI", el control 3 que indica lo siguiente "El operador que gestiona el inventario, una vez al año verifica el nivel de obsolescencia de la infraestructura tecnológica mediante comparación

⁵ Business Impact Analysis.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

de información extraída de los módulos Asset Management de la herramienta Aranda y Almacén del sistema STONE. En caso de no hacer la comparación, se pueden hacer análisis (sic) comparativos contra la situación actual del mercado”. Indicaron que se hace el análisis con la solicitud que la OCI efectúa cada año para el seguimiento al cumplimiento de la normatividad de derechos de autor, es decir que en 2022 lo debieron efectuar en marzo.

Allegaron, como soporte, un archivo titulado “ANÁLISIS DE OBSOLESCENCIA DE SERVIDORES FÍSICOS” que presenta 34 elementos con datos de fecha de compra y años de servicio. Para 18 de esos elementos calcularon los años de servicio con valores que oscilan entre 9,5 y 15,7 años. El mismo documento indica que “Se considera que un servidor es obsoleto cuando cumple más de 8 años de servicio” y sugiere “[...] hacer el reemplazo o la migración de la información de los equipos con un mayor grado de obsolescencia: SERVIDOR DE ARCHIVOS HP ML350 y SERVIDORES BLADE 460C G9”, que corresponden a 5 elementos con obsolescencia de 15,7 (el servidores de archivos) y 14,8 años (4 servidores Blade).

Así, se cumplió el requisito de realización del informe. No obstante, en el documento no se evidencia cuándo exactamente fue realizado el análisis, aunque con base en los datos de fecha de compra y años de servicio, se pudo determinar que éste se efectuó en diciembre de 2022, posterior a la fecha de la entrevista de auditoría (02/12/2022) y no en marzo de 2022, como mencionaron. Dado que no está establecida una fecha exacta para la realización de este análisis, no se genera un hallazgo de auditoría, pero se hace la recomendación de establecer un periodo de tiempo específico, que podría ser un mes o trimestre, según sea pertinente, para asegurar que cada año, en las mismas fechas, se realice la verificación del nivel de obsolescencia de los elementos de TI y que ésta contribuya a la toma de decisiones relacionadas con la gestión de la capacidad.

Como parte de lo relacionado con gestión de la capacidad, se revisó el control “El grupo de Infraestructura de la Subdirección Técnica de Recursos Tecnológicos, (sic) realiza la verificación de la vida útil del activo”, planteado para el riesgo de Seguridad de la Información (SI) identificado como I.02 “Pérdida de integridad y disponibilidad en los Servidores físicos del centro de cómputo (Incluye Sistema Operativo) [...]” del proceso de Gestión de TIC. Dicho control está planteado para la vulnerabilidad de “Obsolescencia no controlada de los recursos tecnológicos” y en la matriz de riesgos de SI está indicado que el registro es “Hoja de vida del activo”.

El personal de la STRT presentó un archivo “HV SERVIDORES 2022.xlsx” que se encuentra en un Drive y registraba como última actualización el 30/09/2022. No obstante, se observó que faltan datos en algunas de las fichas, como es el caso del servidor físico WS02CC01 (ver imagen N° 6). Adicionalmente, el formato –que no forma parte de la documentación del Sistema Integrado de Gestión MIPG-SIG, por lo cual no tiene código– no contempla un campo que indique la fecha de diligenciamiento o actualización ni quién hizo el diligenciamiento.

Respecto a esta situación no se genera un hallazgo puesto que, aunque pudiera ser obvio, el control no especifica cada cuánto o en qué circunstancias se hace el diligenciamiento o actualización. Adicionalmente, como parte del alcance de la prueba de auditoría efectuada no se verificaron, uno a uno, los registros para determinar qué información podría o no ser aplicable dependiendo del elemento. Se recomienda, entonces, completar la información del formato lo más pronto posible e incluir información de trazabilidad del diligenciamiento de cada ficha, agregando, para aquellos activos en los que no aplique cierta información, un dato que permita inferirlo.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Imagen N.º 6. Vista de una ficha del formato de Hoja de Vida de Servidores 2022

		HOJA DE VIDA SERVIDORES		CÓDIGO	
				VERSIÓN	1
				FECHA DE PUBLICACIÓN	
1. Nombre WS02CC01		2. Físico / Virtual Físico		3. Ubicación	
4. Marca		5.1 Referencia		6. Serial	
8. sistema operativo MICROSOFT WINDOWS SERVER 2012		Cantidad de Memoria		Procesador	
				7. Placa discos	
				9. Tipo de adquisición	
				10. Contrato	
11. Fecha fin garantía		11.1. Fecha ampliación garantía		12. Fecha de baja	
13. Despliegues o Aplicaciones 13.1. Servicios CONSOLA		13.2. Direcciónamiento IP 172.16.31.9		13. Despliegues o Aplicaciones 13.1. Servicios WSUS	
				13.2. Direcciónamiento IP	
HISTORIAL DE MANTENIMIENTOS					
 WS02CC01 - AV03CC01 - AV04CC01 - BI01CC01 - BK01CC01 - BK03CC01 - BS01CC01 -					

Fuente: Pantallazo obtenido de la entrevista de auditoría del 02/12/2022.

De acuerdo con lo descrito, se puede concluir que el proceso está midiendo la gestión de la capacidad, que está haciendo uso del formato FO-TI-30 “Control de la capacidad”, versión 1, que se encuentra vigente y que está realizando gestiones para mejorar la automatización para el diligenciamiento del formato, efectuada en 2021 en razón de una acción de mejoramiento planteada por el proceso. No obstante, se evidenció que la automatización inicialmente desarrollada no se utilizó en la mayor parte de 2022, dado que el registro de la información en los primeros trimestres se hizo manual y sólo para servidores de almacenamiento; la herramienta automatizada se retomó a partir septiembre de 2022 y es aún un piloto.

Lo anterior indica que la acción de mejora 2523 “Diligenciar el formato FO-TI-30 de manera automatizada, mediante la creación de un componente tecnológico, que tome la información de capacidad del SIEM” resulta inefectiva dado que se desarrolló y estuvo inutilizada por los menos por 8 meses. Esto se constituye en un hallazgo de auditoría.

Adicionalmente, se evidenció incumplimiento de la periodicidad de toma de las mediciones de control de la capacidad y debilidades en el diligenciamiento del FO-TI-30, puesto que lo registrado, al menos para

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

los 3 primeros trimestres no se efectuó en los 5 primeros días hábiles de cada periodo, como lo establece el procedimiento vigente. Esto da lugar a un hallazgo de auditoría.

Es importante mencionar que los cuatro términos (Capacidad, Capacidad Nominal, Capacidad Real y Umbral), relacionados del numeral 1.4. “*Términos y Definiciones*” del procedimiento PR-TI-16, versión 3, no se encontraron en el diccionario de términos IDU. Además, en la política operacional 5 está referida la actividad “1.1.6.2 *identificarla (sic) capacidad actual*”, la cual no existe en el citado procedimiento, porque el numeral correcto es “1.6.2. *Identificar la capacidad actual*”.

2. Copia de respaldo ordinaria

Si bien no se encontró la definición, las copias de respaldo ordinarias son las que realizan para elementos de información de alta relevancia para el Instituto, como es el caso de las bases de datos, los sistemas de información, archivos compartidos, entre otros. Para la copia de respaldo ordinaria, la STRT tiene establecida una programación que, de acuerdo con lo indicado en la política operacional del manual operativo MG-TI-016 “*Manual Backups y Recuperación de la Información*”, en el caso de las bases de datos, se puede resumir como sigue:

Tabla N.º 6. Políticas de periodicidad de copiado

Base de datos	Periodicidad de copiado desde los servidores de Base de Datos:	Periodicidad de copiado desde la herramienta de Backup:
Oracle	<ul style="list-style-type: none"> • Backup Nivel 0: Diario 1 vez al día iniciando 21:00 terminando a las 07:00. • Backup Archivelog RMAN: Diario 1 vez al día iniciando 20:00 terminando 	<ul style="list-style-type: none"> • Backup Nivel 0: Mensual total últimos 3 días del mes. • Backup incremental Nivel 1: Diario (inicia 10:00)
SQLSERVER (sic)	<ul style="list-style-type: none"> • Backup FULL con LOG: Diario 2 vez al día, uno a las 00:00 y el otro a las 12:00. 	<ul style="list-style-type: none"> • Backup Nivel 0: Mensual total últimos 3 días del mes. • Backup incremental Nivel 1: Diario (inicia 10:00)
OPEN SOURCE (MariaDB, MySQL, POSTGRESQL)	<ul style="list-style-type: none"> • Backup FULL: Diario 2 vez al día, uno entre 23:30 y 00:30 y el otro entre las 11:30 y las 12:30. 	<ul style="list-style-type: none"> • Backup Nivel 0: Mensual total últimos 3 días del mes. • Backup incremental Nivel 1: Diario (inicia 10:00 am)

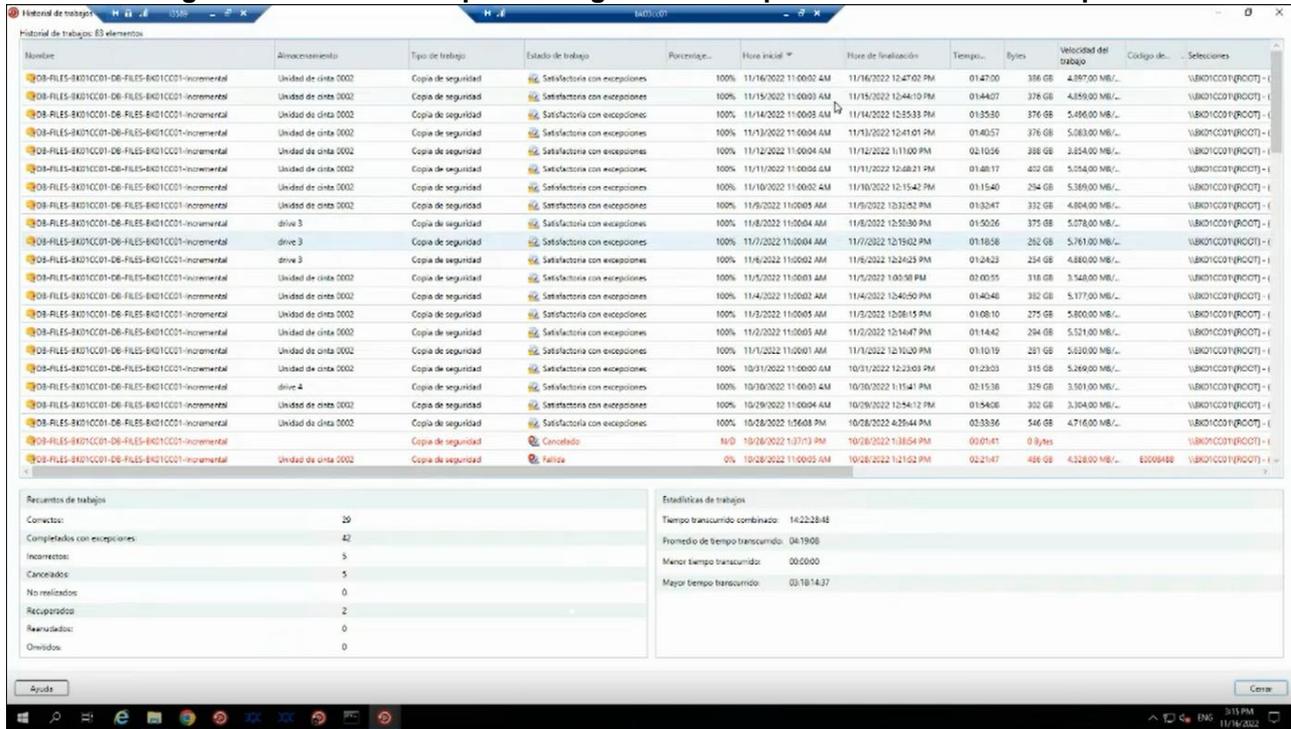
Fuente: Manual Operativo MG-TI-016. **Elaboración:** Equipo Auditor.

El proceso de copia de bases de datos se está realizando, inicialmente, a un servidor específico (BK01CC01) y posteriormente, a través de la herramienta de *backup* se aplica la política citada en la tabla anterior. El personal del proceso explicó que esta decisión se tomó para optimizar el proceso de copias de seguridad y reducir problemas tales como lentitud en los sistemas de información o en la generación de la copia de seguridad.

Es de mencionar que se evidenció una diferencia de una hora para algunos de los *backups* incrementales, en los horarios del manual y la programación en la herramienta, dado que en el primero indican que inician a las 10:00 am, pero en la herramienta se veía que iniciaba a las 11:00 am. Se recomienda revisar la documentación para efectuar el ajuste respectivo y asegurar que las actividades de *backup* que se realizan según como están documentadas. Los *jobs* o tareas de copias de seguridad se visualizan así en la herramienta Veritas Backup Exec, que es la utilizada para el asunto y se aloja en la máquina identificada como BK03CC01:

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Imagen N.º 7. Jobs de copias de seguridad en la plataforma Veritas Backup Exec

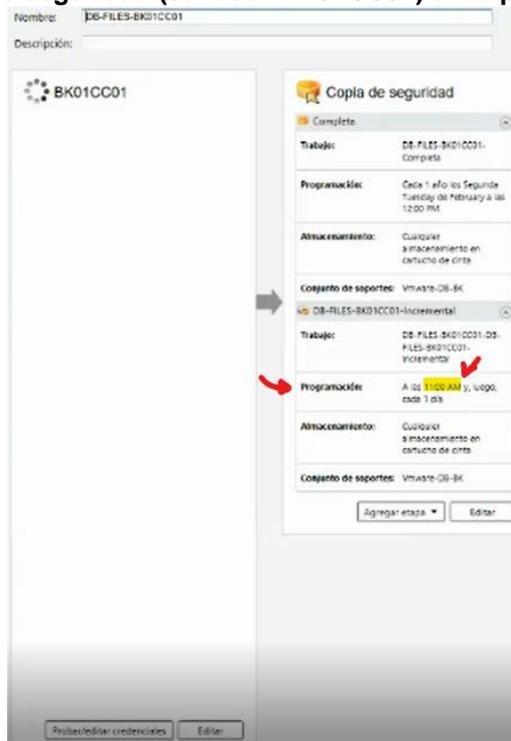


Nombre	Almacenamiento	Tipo de trabajo	Estado de trabajo	Porcentaje	Hora inicial	Hora de finalización	Tiempo	Bytes	Velocidad del trabajo	Código de...	Selecciones
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/16/2022 11:00:02 AM	11/16/2022 12:47:02 PM	01:47:00	386 GB	4.987.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/15/2022 11:00:03 AM	11/15/2022 12:44:10 PM	01:44:07	376 GB	4.859.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/14/2022 11:00:03 AM	11/14/2022 12:35:33 PM	01:35:30	376 GB	5.496.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/13/2022 11:00:04 AM	11/13/2022 12:41:01 PM	01:40:57	376 GB	5.083.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/12/2022 11:00:04 AM	11/12/2022 11:11:00 PM	02:10:56	388 GB	3.854.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/11/2022 11:00:04 AM	11/11/2022 12:48:21 PM	01:48:17	402 GB	5.054.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/10/2022 11:00:02 AM	11/10/2022 12:15:42 PM	01:15:40	294 GB	5.369.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/9/2022 11:00:05 AM	11/9/2022 12:32:52 PM	01:32:47	332 GB	4.804.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	drive 3	Copia de seguridad	Satisfactoria con excepciones	100%	11/8/2022 11:00:04 AM	11/8/2022 12:50:30 PM	01:50:26	375 GB	5.078.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	drive 3	Copia de seguridad	Satisfactoria con excepciones	100%	11/7/2022 11:00:04 AM	11/7/2022 12:15:02 PM	01:15:58	262 GB	5.761.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	drive 3	Copia de seguridad	Satisfactoria con excepciones	100%	11/6/2022 11:00:02 AM	11/6/2022 12:24:25 PM	01:24:23	254 GB	4.860.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/5/2022 11:00:03 AM	11/5/2022 1:00:50 PM	03:00:55	318 GB	3.548.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/4/2022 11:00:02 AM	11/4/2022 12:40:50 PM	01:40:46	382 GB	5.177.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/3/2022 11:00:05 AM	11/3/2022 12:08:15 PM	01:08:10	275 GB	5.800.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/2/2022 11:00:05 AM	11/2/2022 12:14:47 PM	01:14:42	294 GB	5.521.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	11/1/2022 11:00:01 AM	11/1/2022 12:10:20 PM	01:10:19	281 GB	5.830.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	10/31/2022 11:00:00 AM	10/31/2022 12:23:03 PM	01:23:03	315 GB	5.249.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	drive 4	Copia de seguridad	Satisfactoria con excepciones	100%	10/30/2022 11:00:03 AM	10/30/2022 1:11:41 PM	02:15:38	329 GB	3.501.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	10/29/2022 11:00:04 AM	10/29/2022 12:54:12 PM	01:54:06	302 GB	3.304.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Satisfactoria con excepciones	100%	10/28/2022 11:56:08 PM	10/28/2022 4:26:44 PM	02:30:36	546 GB	4.716.00 MB/s	VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Cancelado	N/D	10/28/2022 13:17:13 PM	10/28/2022 1:38:54 PM	00:01:41	0 bytes		VBK01CC01(FRCOT)-I	
DB-FILES-BK01CC01-DB-FILES-BK01CC01-Incremental	Unidad de cinta 0002	Copia de seguridad	Fallida	0%	10/28/2022 11:00:02 AM	10/28/2022 12:21:52 PM	02:21:47	486 GB	4.328.00 MB/s	E008498	VBK01CC01(FRCOT)-I

Recuentos de trabajos		Estadísticas de trabajos	
Correctos:	20	Tiempo transcurrido combinado:	14:22:28.48
Completados con excepciones:	42	Promedio de tiempo transcurrido:	04:19:08
Incorrectos:	5	Menor tiempo transcurrido:	00:00:00
Cancelados:	5	Mayor tiempo transcurrido:	03:18:14.37
No realizados:	0		
Recuperados:	2		
Reanudados:	0		
Omitidos:	0		

Fuente: Pantallazo obtenido de la entrevista de auditoría del 16/11/2022.

Imagen N.º 8. Job de copia de seguridad (servidor BK01CC01) en la plataforma Veritas Backup Exec



Fuente: Pantallazo obtenido de la entrevista de auditoría del 16/11/2022.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

También se identificó que se hace copia de seguridad de los servidores de archivos y recursos compartidos y de los servidores virtualizados. En el caso del correo electrónico se hace uso del servicio Google Vault.

La programación de toma de las copias de seguridad se realiza en la herramienta de *backups* según lo establecido en la manual de copias de seguridad. La herramienta de copias de seguridad genera alertas para determinar si las copias fueron realizadas correctamente o no. En el listado de tareas y en el histórico que mantiene la herramienta es posible determinar cuáles tareas no se llevaron a cabo correctamente y si se volvieron a lanzar.

Imagen N.º 9. Ejemplo de la programación de Backups (una semana) en la plataforma Veritas Backup Exec



13 Sunday	14 Monday	15 Tuesday	16 Wednesday	17 Thursday	18 Friday	19 Saturday
Satisfactoria con excepciones S3-MAR-SS04CC01_ARCHIVOS -Increment Copia de seguridad 11/13/2022 12:00:04 AM 11/13/2022 12:00:04 AM 00:06:30 172 MB 430.00 MB/min.	Satisfactoria con excepciones S3-MAR-SS04CC01_ARCHIVOS -Increment Copia de seguridad 11/14/2022 12:00:03 AM 11/14/2022 12:06:31 AM 00:06:28 172 MB 530.00 MB/min.	Satisfactoria con excepciones S3-MAR-SS04CC01_ARCHIVOS -Increment Copia de seguridad 11/15/2022 12:00:03 AM 11/15/2022 12:06:05 AM 00:06:16 207 MB 27.00 MB/min.	Satisfactoria con excepciones S3-MAR-SS04CC01_ARCHIVOS -Increment Copia de seguridad 11/16/2022 12:00:01 AM 11/16/2022 12:06:16 AM 00:06:23 207 MB 592.00 MB/min.	Satisfactoria con excepciones S3-MAR-SS04CC01_ARCHIVOS -Increment Copia de seguridad 11/17/2022 12:00:01 AM 11/17/2022 12:06:25 AM 00:06:24 422 MB 694.00 MB/min.	Satisfactoria con excepciones S3-MAR-SS04CC01_ARCHIVOS -Increment Copia de seguridad 11/18/2022 12:00:00 AM 11/18/2022 12:06:53 AM 00:06:53 447 MB 696.00 MB/min.	Satisfactoria con excepciones S3-MAR-SS04CC01_ARCHIVOS -Increment Copia de seguridad 11/19/2022 12:00:02 AM 11/19/2022 12:06:23 AM 00:06:21 280 MB 671.00 MB/min.
Satisfactoria con excepciones S4-FEB-FS06CC01_ARCHIVOS_J-L-Increment Copia de seguridad 11/13/2022 12:00:05 AM 11/13/2022 12:06:20 AM 00:06:15 829 Bytes 0.00 MB/min.	Satisfactoria con excepciones S4-FEB-FS06CC01_ARCHIVOS_J-L-Increment Copia de seguridad 11/14/2022 12:00:04 AM 11/14/2022 12:07:22 AM 00:07:18 35.1 MB 525.01 MB/min.	Satisfactoria con excepciones S4-FEB-FS06CC01_ARCHIVOS_J-L-Increment Copia de seguridad 11/15/2022 12:00:04 AM 11/15/2022 12:05:38 AM 00:05:34 839 Bytes 0.00 MB/min.	Satisfactoria con excepciones S4-FEB-FS06CC01_ARCHIVOS_J-L-Increment Copia de seguridad 11/16/2022 12:00:01 AM 11/16/2022 12:10:45 AM 00:10:44 11.1 GB 5.648.18 MB/min.	Satisfactoria con excepciones S4-FEB-FS06CC01_ARCHIVOS_J-L-Increment Copia de seguridad 11/17/2022 12:00:03 AM 11/17/2022 12:10:50 AM 00:10:47 19.0 GB 5.927.00 MB/min.	Satisfactoria con excepciones S4-FEB-FS06CC01_ARCHIVOS_J-L-Increment Copia de seguridad 11/18/2022 12:00:01 AM 11/18/2022 12:10:12 AM 00:10:11 695 MB 5.264.02 MB/min.	Satisfactoria con excepciones S4-FEB-FS06CC01_ARCHIVOS_J-L-Increment Copia de seguridad 11/19/2022 12:00:04 AM 11/19/2022 12:10:31 AM 00:10:27 34.1 MB 1.022.02 MB/min.
Satisfactoria con excepciones S4-ENE-FS06CC01_ARCHIVOS_G-INCREM Copia de seguridad 11/13/2022 12:00:06 AM 11/13/2022 12:04:18 AM 00:04:12 364 Bytes 0.00 MB/min.	Satisfactoria con excepciones S4-ENE-FS06CC01_ARCHIVOS_G-INCREM Copia de seguridad 11/14/2022 12:00:05 AM 11/14/2022 12:04:17 AM 00:04:06 364 Bytes 0.00 MB/min.	Satisfactoria con excepciones S4-ENE-FS06CC01_ARCHIVOS_G-INCREM Copia de seguridad 11/15/2022 12:00:05 AM 11/15/2022 12:04:37 AM 00:04:32 1.52 GB 4.664.00 MB/min.	Satisfactoria con excepciones S4-ENE-FS06CC01_ARCHIVOS_G-INCREM Copia de seguridad 11/16/2022 12:00:02 AM 11/16/2022 12:06:25 AM 00:06:23 936 MB 2.954.00 MB/min.	Satisfactoria con excepciones S4-ENE-FS06CC01_ARCHIVOS_G-INCREM Copia de seguridad 11/17/2022 12:00:02 AM 11/17/2022 12:07:20 AM 00:07:15 3.63 GB 2.971.00 MB/min.	Satisfactoria con excepciones S4-ENE-FS06CC01_ARCHIVOS_G-INCREM Copia de seguridad 11/18/2022 12:00:01 AM 11/18/2022 12:06:29 AM 00:06:27 3.09 GB 3.453.00 MB/min.	Satisfactoria con excepciones S4-ENE-FS06CC01_ARCHIVOS_G-INCREM Copia de seguridad 11/19/2022 12:00:06 AM 11/19/2022 12:05:17 AM 00:05:11 130 MB 1.949.01 MB/min.
Satisfactoria con excepciones S2-ENE-S2-ENE-BODEGA_ORFEO_2018_IN Copia de seguridad 11/13/2022 12:00:06 AM 11/13/2022 12:06:52 AM 00:06:44 25.4 KB 0.00 MB/min.	Satisfactoria con excepciones S2-ENE-S2-ENE-BODEGA_ORFEO_2018_IN Copia de seguridad 11/14/2022 12:00:06 AM 11/14/2022 12:04:54 AM 00:04:48 25.4 KB 0.00 MB/min.	Satisfactoria con excepciones S2-ENE-S2-ENE-BODEGA_ORFEO_2018_IN Copia de seguridad 11/15/2022 12:00:07 AM 11/15/2022 12:06:44 AM 00:06:37 25.4 KB 0.00 MB/min.	Satisfactoria con excepciones S2-ENE-S2-ENE-BODEGA_ORFEO_2018_IN Copia de seguridad 11/16/2022 12:00:04 AM 11/16/2022 12:06:50 AM 00:06:46 1.10 MB 1.00 MB/min.	Satisfactoria con excepciones S2-ENE-S2-ENE-BODEGA_ORFEO_2018_IN Copia de seguridad 11/17/2022 12:00:06 AM 11/17/2022 12:09:41 AM 00:09:35 25.4 KB 0.00 MB/min.	Satisfactoria con excepciones S2-ENE-S2-ENE-BODEGA_ORFEO_2018_IN Copia de seguridad 11/18/2022 12:00:03 AM 11/18/2022 12:10:11 AM 00:10:08 25.4 KB 0.00 MB/min.	Satisfactoria con excepciones S2-ENE-S2-ENE-BODEGA_ORFEO_2018_IN Copia de seguridad 11/19/2022 12:00:08 AM 11/19/2022 12:09:42 AM 00:09:34 0.00 MB/min.
Satisfactoria con excepciones S3-MAR-S3-MAR-BODEGA_ORFEO_2013_IN Copia de seguridad 11/13/2022 12:00:09 AM 11/13/2022 12:06:33 AM 00:06:24 31.0 KB 0.00 MB/min.	Satisfactoria con excepciones S3-MAR-S3-MAR-BODEGA_ORFEO_2013_IN Copia de seguridad 11/14/2022 12:00:07 AM 11/14/2022 12:05:59 AM 00:05:52 31.0 KB 0.00 MB/min.	Satisfactoria con excepciones S3-MAR-S3-MAR-BODEGA_ORFEO_2013_IN Copia de seguridad 11/15/2022 12:00:08 AM 11/15/2022 12:09:18 AM 00:09:10 31.0 KB 0.00 MB/min.	Satisfactoria con excepciones S3-MAR-S3-MAR-BODEGA_ORFEO_2013_IN Copia de seguridad 11/16/2022 12:00:06 AM 11/16/2022 12:09:48 AM 00:09:42 1.10 MB 0.00 MB/min.	Satisfactoria con excepciones S3-MAR-S3-MAR-BODEGA_ORFEO_2013_IN Copia de seguridad 11/17/2022 12:00:09 AM 11/17/2022 12:09:57 AM 00:09:49 1.10 MB 0.00 MB/min.	Satisfactoria con excepciones S3-MAR-S3-MAR-BODEGA_ORFEO_2013_IN Copia de seguridad 11/18/2022 12:00:04 AM 11/18/2022 12:10:13 AM 00:10:09 31.0 KB 0.00 MB/min.	Satisfactoria con excepciones S3-MAR-S3-MAR-BODEGA_ORFEO_2013_IN Copia de seguridad 11/19/2022 12:00:09 AM 11/19/2022 12:09:50 AM 00:09:41 31.0 KB 0.00 MB/min.
Satisfactoria con excepciones S2-FEB-FS06CC01_ARCHIVOS_HH-Increment Copia de seguridad 11/13/2022 12:00:10 AM 11/13/2022 12:09:17 AM 00:09:07 178 MB 1.768.67 MB/min.	Satisfactoria con excepciones S2-FEB-FS06CC01_ARCHIVOS_HH-Increment Copia de seguridad 11/14/2022 12:00:08 AM 11/14/2022 12:08:44 AM 00:09:36 200 MB 2.416.82 MB/min.	Satisfactoria con excepciones S2-FEB-FS06CC01_ARCHIVOS_HH-Increment Copia de seguridad 11/15/2022 12:00:11 AM 11/15/2022 12:09:18 AM 00:09:08 890 KB 25.06 MB/min.	Satisfactoria con excepciones S2-FEB-FS06CC01_ARCHIVOS_HH-Increment Copia de seguridad 11/16/2022 12:00:07 AM 11/16/2022 12:13:32 AM 00:13:25 3.50 GB 1.746.71 MB/min.	Satisfactoria con excepciones S2-FEB-FS06CC01_ARCHIVOS_HH-Increment Copia de seguridad 11/17/2022 12:00:10 AM 11/17/2022 12:13:32 AM 00:13:23 409 MB 2.955.66 MB/min.	Satisfactoria con excepciones S2-FEB-FS06CC01_ARCHIVOS_HH-Increment Copia de seguridad 11/18/2022 12:00:04 AM 11/18/2022 12:14:11 AM 00:14:07 6.51 GB 2.955.66 MB/min.	Satisfactoria con excepciones S2-FEB-FS06CC01_ARCHIVOS_HH-Increment Copia de seguridad 11/19/2022 12:00:10 AM 11/19/2022 12:11:35 AM 00:11:25 345 MB 1.034.81 MB/min.
Satisfactoria con excepciones ArcGIS-Vmware-Incremental Copia de seguridad 11/13/2022 12:00:13 AM 11/13/2022 12:41:00 AM 00:41:55 16.0 GB 698.98 MB/min.	Satisfactoria con excepciones ArcGIS-Vmware-Incremental Copia de seguridad 11/14/2022 12:00:12 AM 11/14/2022 12:41:41 AM 00:41:29 15.7 GB 670.48 MB/min.	Satisfactoria con excepciones ArcGIS-Vmware-Incremental Copia de seguridad 11/15/2022 12:00:18 AM 11/15/2022 12:42:08 AM 00:41:50 16.5 GB 694.36 MB/min.	Satisfactoria con excepciones ArcGIS-Vmware-Incremental Copia de seguridad 11/16/2022 12:00:11 AM 11/16/2022 12:57:03 AM 00:45:52 23.1 GB 613.40 MB/min.	Satisfactoria con excepciones ArcGIS-Vmware-Incremental Copia de seguridad 11/17/2022 12:00:15 AM 11/17/2022 12:47:00 AM 00:45:45 17.8 GB 642.65 MB/min.	Satisfactoria con excepciones ArcGIS-Vmware-Incremental Copia de seguridad 11/18/2022 12:00:09 AM 11/18/2022 12:48:27 AM 00:48:18 19.6 GB 224.22 MB/min.	Fallida ArcGIS-Vmware-Incremental Copia de seguridad 11/19/2022 12:00:14 AM 11/19/2022 12:05:14 AM 00:05:00 21.6 GB 206.27 MB/min.

Fuente: STRT.

Para el almacenamiento en disco utilizan la máquina identificada como DELL – DR6000 y para el almacenamiento en cinta están dispuestas las máquinas de librerías de cintas magnéticas⁶ identificadas como LTO 6 y LTO 6 – LTO-7 – LTO-8.

De acuerdo con lo explicado por el personal del proceso, las copias de seguridad permanecen en el equipo DR6000 durante 6 meses (o más). No obstante, se determinó que, en los jobs “S3-MAR-BODEGA_ORFEO_2013” y “D1-BK03CC01_DB_BKEXEC”, el parámetro en la configuración está por debajo, dado que está configurado como 18 semanas, lo que equivaldría a 4,5 meses.

En el caso de las cintas que se llenen, se almacenan, inicialmente en la cintoteca del IDU, en donde permanecen, también, mínimo 6 meses y posteriormente son trasladadas, por transferencia documental, a la Subdirección de Recursos Físicos - STRF para la custodia externa. Se evidenció que la más reciente transferencia la efectuaron el 22/11/2022 en la que fueron entregados 59 medios magnéticos al archivo central del IDU. Posteriormente, la STRF se encarga de efectuar el paso a custodia externa, para lo cual

⁶ Conocidas como LTO: Linear Tape-Open.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

está en ejecución el contrato IDU-1659-2021 con la firma TANDEM S.A.S. Es de aclarar que el contrato no es de exclusividad para medios magnéticos de la STRT, sino es para almacenamiento y custodia de archivos y medios magnéticos de todo el Instituto.

Dentro de las actividades a realizar por el operador de copias de seguridad y base de datos está la de “Presentar al Subdirector, informes de estado de los trabajos de copias de seguridad y restauración realizados, de forma bimestral”. Se pudo establecer que se efectúan reportes a la subdirectora, pero no con la periodicidad indicada. Por ejemplo, se evidenciaron Reportes de Monitoreo de Plataforma Backups IDU del 30/09/2022 y del 13/11/2022, realizados por la Unión Temporal Backup IT 2022 en el marco del contrato IDU-514-2022 cuyo objeto es la “renovación del soporte y garantías de la solución de backup que respalda el proceso de copias de seguridad y adquisición de una plataforma complementaria de backup para el Instituto de Desarrollo Urbano”, pero estos corresponden a reportes diarios y no son elaborados por el operador de copias de seguridad. También se evidenció un correo en el que uno de los responsables del tema de copias de seguridad informa que efectuó revisión de los jobs fallidos y los envió a ejecución.

No fue posible establecer si adicional a estos reportes diarios se efectúan los bimestrales, tampoco que incluyan información de trabajos de restauración. Esto genera un hallazgo de auditoría.

3. Copia de respaldo por demanda

Se verificó que, según solicitud de los usuarios del Instituto, el proceso de Gestión TIC puede generar copias de seguridad de información o elementos específicos. Para ello está establecido el formato FO-TI-218 “Solicitud de Realización de Backup”. El formato puede ser remitido por correo electrónico institucional a la STRT y debe estar aprobado por el jefe del área que solicita y por el jefe de la STRT. No fue posible identificar, en las pruebas de auditoría efectuadas, si durante la vigencia se realizaron *backups* a demanda.

Se pudo evidenciar que, en el caso de solicitudes efectuadas por el mismo personal de la STRT, por ejemplo, para pruebas de desarrollos propios no era exigido. Por tanto, se recomienda documentar las excepciones para el uso de este formato.

4. Información restaurada

Se verificó que el proceso ha efectuado la restauración de copias de seguridad, pero no obedeciendo al plan de pruebas, sino a demanda. De hecho, se verificó que no existe el plan de pruebas de restauración o la realización de pruebas periódicas aleatorias para garantizar que las copias de seguridad funcionan correctamente y la información contenida es recuperable. Esto constituye un hallazgo de auditoría.

Ahora bien, en el caso de las restauraciones a demanda, se pudo evidenciar la utilización del formato FO-TI-185 “Solicitud de Restauración de Backup” en una solicitud de la Subdirección General de Desarrollo Urbano, mas se pudo establecer que en los casos solicitados por personal de la misma STRT no se exigió el mismo. Es de anotar que estas solicitudes fueron de aplicativos como Stone y Kactus para efectos de pruebas o verificaciones de información. Por tanto, se recomienda documentar las excepciones para el uso de este formato.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Imagen N.º 10. Ejemplo de *jobs* de restauración de *Backups* en la plataforma Veritas Backup Exec

Trabajos: 9 elementos								
Nombre	Servidor	Almacenamiento	Tipo de trabajo	Estado	Estado de trabajo	Estado de trabajo activo	Bytes	Hora inicial
ss05cc01 Restaurar - SGDU	ss05cc01		Restaurar	Activo	Activo: En cola	00:27:28	0 Bytes 0.00 MB/min.	11/23/2022 9:01:31 PM
ss05cc01 Restaurar 01317	ss05cc01	Biblioteca robótica 0001	Restaurar	programado	En espera			9/29/2022 12:55:21 PM
g08cc01 Restaurar 01057	g08cc01		Restaurar	programado	En espera			9/29/2022 12:55:20 PM
g08cc01 Restaurar 01058	g08cc01	Biblioteca robótica 0001	Restaurar	programado	En espera			9/29/2022 12:55:20 PM
MV02CL01 Restaurar 01122	MV02CL01		Restaurar	programado	En espera			9/29/2022 12:55:20 PM
ORFEO_120161150078243_00002	MV02SV04		Restaurar	programado	En espera			9/29/2022 12:55:20 PM
ss05cc01 GoogleApps 2016 ss05cc01	ss05cc01	Biblioteca robótica 0001	Restaurar	programado	En espera			9/29/2022 12:55:20 PM

Fuente: STRT.

La herramienta permite identificar si el proceso de restauración se llevó a cabo correctamente y los usuarios son los encargados de reportar si los datos quedaron o no correctamente restaurados, esto por cuanto son ellos quienes como propietarios de la información pueden verificarlo.

Actividad crítica “5. Soporte a los Servicios de TI”.

De acuerdo con la caracterización del proceso de Gestión de Tecnologías de Información y Comunicación, esta actividad crítica busca “Atender de forma controlada en un punto centralizado de contacto, las solicitudes de soporte y requerimiento técnicos presentadas por los usuarios de la Entidad, de acuerdo con los niveles de servicio establecidos”. A continuación, se presenta la información correspondiente frente a cada uno de los productos revisados como parte de la presente auditoría:

1. Registro del evento, incidente, problema o requerimiento atendido, solucionado y cerrado

Se verificó que el proceso cuenta con el sistema Aranda para que los usuarios registren los casos o solicitudes de soporte técnico y los eventos o incidentes de seguridad de la información. Como opción, en caso de no acceder al sistema Aranda directamente, los usuarios pueden reportar el caso al correo helpdesk@idu.gov.co o a través de la extensión telefónica 1444. Para el caso de solicitudes de permisos sobre aplicativos la STRT desarrolló, sobre la plataforma de código abierto Odoo, el aplicativo CHIE: Gestión TIC, mediante la cual se asegura que los jefes de las áreas aprueben esas solicitudes. Es de anotar que una vez efectuada esa aprobación, se hace creación de casos en Aranda.

El grupo de mesa de ayuda es el que inicialmente atiende los casos y si es necesario, se hace escalamiento de los casos a niveles superiores como los grupos de desarrollo o infraestructura.

Para efectos de la revisión se solicitó al proceso un listado de casos registrados en agosto de 2022. La STRT allegó un archivo con 5.531 registros, así:

Tabla N.º 7. Cantidad de casos registrados en Aranda – agosto de 2022

Etiquetas de fila	GRUPO ESPECIALISTA	Anulado	Cerrado	Solucionado	Total general
CAMBIOS	Arquitectura	1			1
	Desarrollo - Orfeo		3	1	4
	Desarrollo - Stone		4		4
	Desarrollo - Valoricemos		20		20
LLAMADA DE SERVICIO	Desarrollo		528		528
	Desarrollo - Intranet		28		28

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Etiquetas de fila	GRUPO ESPECIALISTA	Anulado	Cerrado	Solucionado	Total general
	Desarrollo - Kactus		128		128
	Desarrollo - Orfeo		637		637
	Desarrollo - Stone		275		275
	Desarrollo - Valora		2		2
	Desarrollo - Valoricemos		342		342
	Gesin		309		309
	Gestión Administrativa		1		1
	Helpdesk		2.404		2.404
	I+D+I		20		20
	Infraestructura	1	794		795
	Soporte Tecnológico (sic)		33		33
	Total general	2	5.528	1	5.531

Fuente: STRT. Resumen: Equipo auditor.

Como se observa, la mayor cantidad de casos (99,9 %) se encontraba cerrada, así: 5.046 fueron cerrados en agosto de 2022, es decir, el mismo mes de registro, 396 fueron cerrados en septiembre, 74 en octubre y 14 en noviembre de dicho año. Esto significa que la acción de mejora 2521 cumplió su objetivo de “Realizar control al ciclo de vida de casos registrados en el sistema Aranda”.

Con la misma información se verificó la información de los tiempos de atención comparándolos con los señalados en el documento DU-TI-01 “Catálogo de Servicios de Tecnologías de la Información”, que son como siguen:

Tabla N.º 8. Servicios del “Catálogo de Servicios de Tecnologías de la Información” (*)

#	Servicio	Operación Normal		Operación Contingencia	
		Tiempo de Atención	Tiempo de Solución	Tiempo de Atención	Tiempo de Solución
1	Servicio atención de eventos de tecnología	30	120	60	240
2	Servicio instalación de aplicaciones de software	30	240	60	360
3	Servicio soporte sobre aplicaciones de software	30	120	60	240
		30	240	60	360
4	Servicio préstamo de equipos para reuniones	30	240	N/A	N/A
5	Servicio préstamo sala Iducate	30	240	N/A	N/A
6	Servicio digitalización de documentos e impresión en gran formato	30	240	45	180
7	Servicio administración de usuarios de tecnología	30	240	120	2.160 (**)
8	Servicio recursos compartidos	30	240	N/A	N/A
9	Servicio acceso seguro a la red institucional	30	120	60	360
		30	240	60	480
10	Servicio asignación de permiso de navegación en internet	30	240	120	480
11	Servicio configuración de dispositivos móviles	30	240	45	120
12	Servicio plataforma tecnológica para capacitación virtual	30	240	N/A	N/A
13	Servicio generación de copias de seguridad por demanda	30	240	60	360
14	Servicio restauración de copia de seguridad por demanda	30	240	60	360
15	Servicio acompañamiento en la formulación y desarrollo de proyectos institucionales en el componente de TI	30	240	N/A	N/A

Fuente: DU-TI-01 “Catálogo de Servicios de Tecnologías de la Información”. Resumen: Equipo auditor.

(*) tiempos en minutos. (**) El catálogo registra 36 horas.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Es de mencionar que en el caso de los servicios “*Servicio soporte sobre aplicaciones de software*” y “*Servicio acceso seguro a la red institucional*” presentas dos diferentes tiempos de solución, tanto en operación normal como en contingencia. También, en el “*Servicio digitalización de documentos e impresión en gran formato*” llama la atención que el tiempo de solución en contingencia sea inferior al tiempo en operación normal. Se recomienda, entonces, revisar estos tiempos y efectuar los ajustes pertinentes para evitar ambigüedades.

Para los cálculos efectuados se tuvo en cuenta que el horario laboral oficial del IDU es de 7:00 am a 4:30 pm y que, generalmente se trabaja sólo de lunes a viernes. Inicialmente, sólo se tuvieron en cuenta aquellos registros de “*Llamada de Servicio*”. Dado que en ese mes no hubo operación en contingencia, se determinó que el tiempo de atención debió ser de 30 minutos.

Se encontraron 3.888 casos en los cuales la atención fue extemporánea pues, desde el registro, fueron superados los 30 minutos, con rangos de atención que oscilan desde los 31 minutos hasta los 34.753 minutos. Estos casos, cuya atención fue extemporánea, representan el 70,29 % sobre el total de casos. Cabe anotar que solo 265 de ellos se atendieron en los siguientes 40 minutos al registro (lo que corresponde a 10 minutos más del umbral de media hora) y 430 entre el minuto 41 y la hora después del registro; es decir, que el número de casos atendidos en los siguientes 60 minutos luego del registro del caso fue bajo.

Ahora bien, la información suministrada incluye el campo “*TIEMPOSOLUCION*”. En este campo se encontraron 2.932 casos cuyo tiempo de solución fue superior a 240 minutos, valor que se tomó por ser el más común a los diferentes servicios que presta la STRT en operación normal. Estos casos representan el 53,3 % del total de casos registrados en agosto de 2022 para atención en mesa de ayuda.

Lo anterior significaría que se presentan debilidades en los tiempos de atención y solución de casos, comparados con los establecidos en el catálogo de servicios. Estas situaciones se configuraron en un hallazgo de auditoría.

También se evidenciaron debilidades en la parametrización del aplicativo Aranda, toda vez que en los tiempos de solución estimados (campo “*TIEMPODESOLUCIONESTIMADO*”) aparecen los valores 0, 60, 120, 180, 240 y 420 minutos, pero en el catálogo de servicios no se encuentran 0, ni 420 como ANS válidos. Por otro lado, los valores del catálogo de servicios 360, 480, y 2.160 no se encuentran en la información de parametrización.

Tampoco se evidencia, claramente, en los datos suministrados del mes de agosto, la correspondencia entre los servicios de TI presentados en el Catálogo (ver tabla N° 9) y las jerarquías y/o categorías referidas en la información (ver tabla N° 10).

Tabla N.º 9. Jerarquías y Categorías en el archivo de casos de mesa de ayuda en agosto 2022

JERARQUÍA	CATEGORÍA
Correo.Buzon Interno	Buzon Interno
Correo.Cliente de Correo	Cliente de Correo
Directorio Activo.Dominio	Dominio
Directorio Activo.Estaciones de Trabajo	Estaciones de Trabajo
Hardware.Estaciones de Trabajo.Board	Board
Hardware.Estaciones de Trabajo.Cpu	Cpu
Hardware.Estaciones de Trabajo.Drive CD – DVD	Drive CD - DVD

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

JERARQUÍA	CATEGORÍA
Hardware.Estaciones de Trabajo.Impresora	Impresora
Hardware.Estaciones de Trabajo.Mouse	Mouse
Hardware.Estaciones de Trabajo.Otro Dispositivo	Otro Dispositivo
Hardware.Estaciones de Trabajo.Plotter	Plotter
Hardware.Estaciones de Trabajo.Scanner	Scanner
Hardware.Estaciones de Trabajo.Teclado	Teclado
Hardware.Servidores.Cpu	Cpu
Hardware.Servidores.Otro Dispositivo	Otro Dispositivo
IMPRESIÓN Y DIGITALIZACION.CONFIGURACION DE IMPRESORAS	CONFIGURACION DE IMPRESORAS
IMPRESIÓN Y DIGITALIZACION.DIGITALIZAR DOCUMENTOS	DIGITALIZAR DOCUMENTOS
IMPRESIÓN Y DIGITALIZACION.IMPRESIÓN EN GRAN FORMATO	IMPRESIÓN EN GRAN FORMATO
Red.LAN.Otro	Otro
Red.LAN.Punto de Red	Punto de Red
Seguridad informática.Firewall Corporativo.VPN	VPN
Seguridad informática.Procesos Selectivos.Firewall.VPN	VPN
SERVIDORES.ASIGNACION DE RECURSOS.PROCESAMIENTO	PROCESAMIENTO
SERVIDORES.CONFIGURACION	CONFIGURACION
Software.Software Comercial.Adobe Acrobat	Adobe Acrobat
Software.Software Comercial.Antivirus	Antivirus
Software.Software Comercial.Aranda	Aranda
Software.Software Comercial.ARCGIS	ARCGIS
Software.Software Comercial.Autocad	Autocad
Software.Software Comercial.Internet Explorer	Internet Explorer
Software.Software Comercial.Office	Office
Software.Software Comercial.Oracle	Oracle
Software.Software Comercial.Otros	Otros
Software.Software Comercial.Sistema Operativo	Sistema Operativo
Software.Software Comercial.VPN NetASQ Cliente	VPN NetASQ Cliente
Software.Software Corporativo.Bachue Módulo de Gestión Social Predios	Bachue Módulo de Gestión Social Predios
Software.Software Corporativo.Bachue Módulo Gestión PQRS	Bachue Módulo Gestión PQRS
Software.Software Corporativo.Intranet	Intranet
Software.Software Corporativo.Kactus - Reclut. Selec.	Kactus - Reclut. Selec.
Software.Software Corporativo.Kactus - Self Services	Kactus - Self Services
Software.Software Corporativo.Kactus Aplicacion	Kactus Aplicacion
Software.Software Corporativo.Moodle	Moodle
Software.Software Corporativo.OPEN ERP Bachue	OPEN ERP Bachue
Software.Software Corporativo.OPEN ERP Chie	OPEN ERP Chie
Software.Software Corporativo.OPEN ERP SUE	OPEN ERP SUE
Software.Software Corporativo.OPEN ERP Zipa	OPEN ERP Zipa
Software.Software Corporativo.OpenErp	OpenErp
Software.Software Corporativo.ORFEO - Gestión Documental y Correspondencia	ORFEO - Gestión Documental y Correspondencia
Software.Software Corporativo.Predios	Predios
Software.Software Corporativo.ProntoPago	ProntoPago
Software.Software Corporativo.Registro Financiero del Contrato	Registro Financiero del Contrato
Software.Software Corporativo.SEGPOAI	SEGPOAI

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

JERARQUÍA	CATEGORÍA
Software.Software Corporativo.SI para actualizacion del censo predial	SI para actualizacion (sic) del censo predial
Software.Software Corporativo.SIAC	SIAC
Software.Software Corporativo.SIGES - Obras	SIGES - Obras
Software.Software Corporativo.SIGES - Predios	SIGES - Predios
Software.Software Corporativo.SigPagos	SigPagos
Software.Software Corporativo.Sistema DSPACES	Sistema DSPACES
Software.Software Corporativo.STONE	STONE
Software.Software Corporativo.Transmilenio	Transmilenio
Software.Software Corporativo.Valora	Valora
Software.Software Corporativo.Valoricemos	Valoricemos

Fuente: STRT, archivo "Reporte General de Gestión STRT v2-2022-11-16_09-56-46_Agosto.xlsx". **Resumen:** Equipo auditor.

De acuerdo con lo anterior, se recomienda efectuar una revisión de la parametrización del sistema Aranda para que haya coincidencia entre los servicios y ANS del catálogo de servicios DU-TI-01 con los tiempos estimados y jerarquías / categorías del sistema.

Como parte de la verificación de esta actividad, también se solicitó un listado de usuarios de red activos e inactivos, el cual fue remitido, por la STRT al equipo auditor, el 21/11/2022. También se solicitó, a la Subdirección Técnica de Recursos Humanos (STRH), el listado de funcionarios que hayan ingresado o se hayan retirado de la Entidad en 2022.

Se efectuaron cruces de información y se encontró que todos los funcionarios que ingresaron en 2022 tenían su usuario activo, según las condiciones establecidas para ello, de acuerdo con lo indicado en el numeral 6.1 "Pasos para dar Inicio a la Creación de Usuarios de Red" del instructivo IN-TI-07 "Administración del Directorio Activo". Sin embargo, se encontraron 4 casos de exfuncionarios que aparecían con el usuario de red activo, como se resume en la tabla siguiente:

Tabla N.º 10. Exfuncionarios con usuario de red activo

Identificación	Nombre Exfuncionario	Retiro		Observaciones equipo auditor	
		Fecha	Causa		
13XXX445	Uriel M C	14/07/2022	Renuncia	Permanece en usuarios activos	Caso en Gestión TIC y caso Aranda 509621 para finalización de permisos
19XXX876	Carlos E L R	01/07/2022	Renuncia	Permanece en usuarios activos	No se encontró solicitud de terminación en Gestión TIC
52XXX219	Marcia A B P	08/02/2022	Terminación nombramiento provisional	Permanece en usuarios activos	Caso en Gestión TIC y caso Aranda 485159 para finalización de permisos
79XXX807	Jaime A B	30/10/2022	Fallecimiento	Permanece en usuarios activos	No se encontró solicitud de terminación en Gestión TIC

Fuente: STRT (usuarios de red) y STRH (ingresos y retiros 2022). **Elaboración:** Equipo auditor a partir de cruces de información.

Lo anterior se configuró en un hallazgo de auditoría que fue comunicado en el informe preliminar de auditoría. Como se presenta en el aparte de análisis de respuesta, en respuesta al informe preliminar la STRT presentó la evidencia de solicitud que efectuó la Subdirección Técnica de Recursos Físicos (STRF) para que permaneciera activo el usuario del funcionario fallecido, mientras se reasignaban sus tareas.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Adicionalmente, en la misma respuesta, la STRT señaló que el área encargada de solicitar la terminación del usuario Carlos E L R no efectuó la gestión en el respectivo aplicativo. El equipo auditor verificó que esta afirmación es cierta, como se relacionó en la tabla N.º 10.

Por lo anterior, fue modificado el hallazgo, retirando esos dos casos del mismo y generando la recomendación de efectuarles seguimiento y realizar las gestiones que correspondan para finalizar los respectivos permisos. Los casos referidos a los exfuncionarios Uriel M C y Marcia A B P se mantuvieron en el hallazgo, toda vez que para ellos no fueron presentados argumentos que los desvirtuaran.

Es importante mencionar que el proceso tiene establecido que la gestión de usuarios (solicitud de permisos, modificaciones, cancelaciones, etc.) se realice a través de facilitadores de las diferentes dependencias del IDU, que son designados por los jefes de las mismas. Estos facilitadores son los encargados de registrar en el sistema CHIE: Gestión TIC las solicitudes de creación, terminación, suspensión y modificación de permisos de los usuarios (funcionarios y contratistas).

Se verificó que la herramienta es usada, pero se evidenciaron debilidades en el registro de caso por parte de algunos facilitadores que, posiblemente, desconocen los tipos de solicitudes que se hacen en dicho sistema. Tal es el caso de los contratistas de prestación de servicios que finalizan un contrato y un tiempo después inician uno nuevo. Para este caso, el sistema tiene contemplado el tipo de solicitud “*Reactivación terminación*”; sin embargo, es común que los facilitadores usen el tipo de solicitud “*Creación*” que se usa cuando la persona no ha tenido vinculación con el IDU. Por tanto, se recomienda reforzar la capacitación sobre este sistema, de manera que se propenda porque el tipo de solicitud de cada caso registrado corresponda con la definición establecida.

Actividad crítica “9. Seguimiento a la Gestión”.

A continuación, se presenta la información correspondiente frente a cada uno de los productos revisados como parte de esta actividad crítica:

1. Análisis de la evaluación del servicio

De acuerdo con lo manifestado por el proceso, el análisis de la evaluación del servicio se refiere a la revisión de la respuesta a las encuestas de satisfacción que diligencian los usuarios cuando la atención a un caso o requerimiento, que hayan hecho a la mesa de ayuda, es cerrada. Para esto, el sistema Aranda está configurado para que, automáticamente, desde el correo adminaranda@idu.gov.co remita al correo institucional del usuario un enlace que dirige a una encuesta de 5 preguntas preestablecidas para que el usuario califique. Éstas tienen 4 opciones de respuesta (selección múltiple con única respuesta): Excelente, Bueno, Regular, Malo. Manifiestan que no dejan pregunta de texto libre porque no permiten hacer agrupamientos ni generar estadísticas.

Respecto de la encuesta, se ha evidenciado que solo se puede diligenciar si se está conectado a la red del IDU, así que, para los teletrabajadores, se dificulta efectuar la calificación a menos que se conecten por VPN y, a través de escritorio remoto, a un equipo de la red local del IDU. Se recomienda revisar esta configuración y evaluar la posibilidad de implementar una solución de encuestas que se pueda responder desde cualquier ubicación.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

También se ha evidenciado que el número de encuestas que responden los usuarios es muy bajo. Por ejemplo, como soporte remitieron el archivo “ASDK - Encuestas de Satisfacción por Areas 2022.xlsx” que muestra una relación de 1.516 usuarios a los cuales se les remitieron encuestas entre el 01/07/2022 y el 30/09/2022. De acuerdo con el archivo, fueron remitidas 15.355 y no fue respondida ninguna, aunque la calificación fue de 5 sobre 5.

El resultado del análisis de la evaluación del servicio alimentaría el indicador de “Percepción de la prestación del servicio de soporte de TI”. En el ejemplo anterior, el que no hayan respondido las encuestas no da una idea de la evaluación del servicio. Simplemente, no fue evaluado.

Por tanto, se recomienda al proceso, buscar estrategias que logren el incremento en el número de encuestas respondidas, o maneras diferentes para que se pueda realizar tal evaluación.

2. Indicadores de gestión del proceso analizados

Una vez revisada la información remitida por la STRT, se pudo evidenciar que la dependencia reporta tres tipos de indicadores, a saber: los de gestión interna del área, los registrados en el cuadro de mando y los correspondientes al Plan de Acción-PAE. A continuación, se detalla el análisis a los indicadores internos y en el siguiente numeral se revisaron los otros dos tipos.

De acuerdo con las tablas Excel Formato FO-PE-01 “Caracterización de Indicadores de Gestión y Recolección de Información” correspondientes al segundo y tercer trimestre de 2022, las cuales se sustentan en el documento DU-PE- 18 “Lineamientos operacionales para el despliegue estratégico en el marco del MIPG”, versión 4, numeral 9 “Indicadores de proceso”, complementan los indicadores estratégicos y “[...] serán entendidos como métricas operacionales que facilitan el seguimiento a los asuntos propios del proceso y/o proyectos específicos”, es decir, que el proceso y/o área puede o no definirlos de acuerdo con sus necesidades de seguimiento. Se evidenció que definen 7 indicadores, como se describen a continuación:

- Disponibilidad de los servicios de TI.
- Porcentaje de reservas presupuestales con giros autorizados.
- Porcentaje de Pasivos Exigibles con giros autorizados.
- Porcentaje de oportunidad en cumplimiento de acciones de Plan de mejoramiento externo.
- Porcentaje de oportunidad en cumplimiento de acciones de Plan de mejoramiento Interno.
- Percepción de la prestación del servicio de soporte de TI.
- Derechos de Petición respondidos con oportunidad.

De estos indicadores llama la atención el de “Percepción de la prestación del servicio de soporte de TI”, ya que es similar al mencionado en el Plan Estratégico de Tecnologías de la Información – PETI, Versión 14, cuya denominación es “Percepción de la prestación del servicio de soporte de TI”, debido a que, en ninguno de los dos trimestres informados, con corte al 30/06/22 y 30/09/22, se puede apreciar el nivel de avance del mismo, porque no se reportaron los valores en las tablas Excel remitidas como soporte a la OCI. Así mismo, se pudo establecer que tampoco aparece medición en el documento de seguimiento al PETI, ya que este instrumento solo reporta ejecuciones presupuestales. Por lo anterior, se recomienda realizar las mediciones pertinentes para medir el nivel de satisfacción en la prestación del servicio.

A continuación, se presentan los resultados de estos indicadores con corte al 30 de septiembre de 2022:

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Porcentaje de oportunidad en cumplimiento de acciones de plan de mejoramiento interno: El indicador, según su objetivo, busca “*Medir la oportunidad del cumplimiento de acciones establecidas en el Plan de mejoramiento interno*” y está relacionado con el proceso de Mejoramiento Continuo. Se mide con base en lo registrado en el “*Aplicativo institucional para seguimiento a planes de mejoramiento - CHIE*”. El cumplimiento del indicador fue de 93,33 % dado que la dependencia efectuó oportunamente 14 acciones de 15 que se registraron en el sistema CHIE.

Porcentaje de oportunidad en cumplimiento de acciones de plan de mejoramiento externo: El indicador, según su objetivo, busca “*Medir la oportunidad del cumplimiento de acciones establecidas en el Plan de mejoramiento externo*” y está relacionado con el proceso de Mejoramiento Continuo. Se mide con base en lo registrado en el “*Aplicativo institucional para seguimiento a planes de mejoramiento - CHIE*”, en relación con los planes de mejoramiento que se deriven de ejercicios de auditoría de entes de control como la Contraloría de Bogotá D. C: o la Contraloría General de la República. De acuerdo con la información reportada, se evidenció que la Subdirección Técnica de Recursos Tecnológicos no tuvo planes de mejoramiento con entes externos de control durante los tres primeros trimestres de 2022.

Derechos de Petición respondidos con oportunidad: El indicador, según su objetivo, pretende “Medir la oportunidad en el cumplimiento de los requisitos legales de las respuestas dadas a la ciudadanía a través del sistema Orfeo” y está relacionado con el proceso de Gestión Social y Servicio a la Ciudadanía. Se mide, trimestralmente, con base en el “Reporte sistema Orfeo”. El cumplimiento del indicador fue del 100 % dado que la dependencia respondió oportunamente 8 de los 8 derechos de petición que le fueron asignados hasta el 30 de septiembre de 2022.

Disponibilidad de los servicios de TI. El indicador, según su objetivo, pretende medir el porcentaje de disponibilidad de los servicios de tecnología de información. Su fórmula es “ $(\text{Nro. de horas de disponibilidad de los servicios} / \text{Nro. total horas del periodo}) * 100\%$ ”. Para el trimestre con corte al 30/09/2022, se evidenció disponibilidad del componente tecnológico en consideración a que los servicios de plataforma tecnológica, según la STRT, se brindan con oportunidad y calidad. Durante este periodo se logró una meta del 99,35 % y se ejecutaron actividades de mantenimiento preventivo y correctivo tanto en los componentes del Datacenter institucional como en servidores de procesamiento, almacenamiento, *appliances* de seguridad, equipos activos de red y comunicaciones. Así mismo, se apreció que, en las observaciones del avance del indicador, la STRT mencionó que: “*los dispositivos ambientales, de control y energéticos del Datacenter, se encuentran en óptimas condiciones de funcionamiento y operatividad*”.

Porcentaje de reservas presupuestales con giros autorizados. El objetivo de este indicador es medir el valor de giro de las reservas y se define por la siguiente fórmula “ $((\text{Valor de las autorizaciones de giro acumuladas de las reservas} + \text{liberaciones}) / \text{Valor de reservas presupuestales definitivas del periodo}) * 100\%$ ”, la meta del valor para el tercer trimestre era de \$ 6.631'595.844 y se ejecutaron \$ 6.415'937.824, obteniendo un porcentaje de avance del 96,75%, logrando un grado de avance bueno para la ejecución del presupuesto definitivo de la vigencia en curso para reservas presupuestales de la dependencia.

Percepción de la prestación del servicio de soporte de TI. El objetivo de este indicador es “*Conocer la percepción de la prestación del servicio de soporte tecnológico*”, la cual se mide por el promedio de las calificaciones de las encuestas del servicio de soporte (que es la fuente de datos) / 5. La frecuencia de medición planteada fue trimestral. Sin embargo, solo se evidenció el registro del valor de 111 %, correspondiente al primer trimestre 2022, pero no indica el número de encuestas realizadas. No se evidenció reporte ni análisis para los siguientes trimestres, por lo que se recomienda actualizar los valores correspondientes a cada trimestre sin reportar.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Porcentaje de Pasivos Exigibles con giros autorizados. El indicador, según su objetivo, pretende “Medir el grado de avance de la ejecución del presupuesto definitivo de la vigencia en curso para Pasivos Exigibles a cargo de la dependencia, mediante las autorizaciones de giros, para hacer seguimiento a los pasivos exigibles”. Y se mide con base en la siguiente fórmula: $((\text{Valor de las autorizaciones de giro acumuladas de pasivos exigibles} + \text{liberaciones}) / \text{Valor de pasivos exigibles definitivos del periodo}) \times 100 \%$. La frecuencia de medición planteada fue trimestral y a septiembre de 2022 se había logrado una meta del 100 %, ya que se ejecutaron el total de los \$ 30.945.307 que se tenían programados para el año.

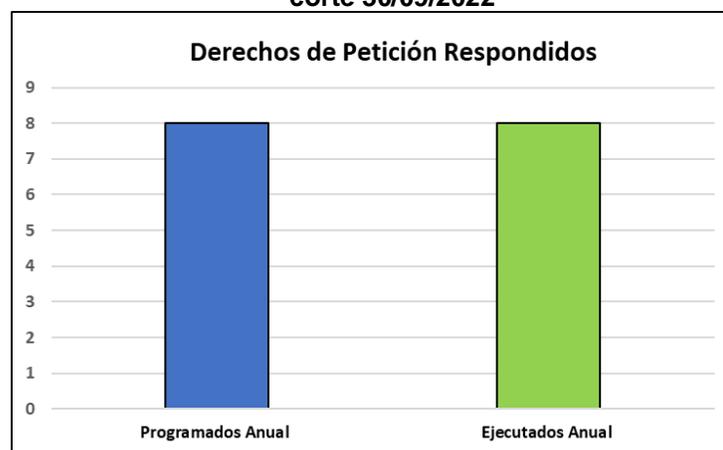
- *Balanced Scorecard - BSC del IDU 2022*

En el *Balanced Scorecard - BSC* del IDU, se encontraron 5 indicadores relacionados con el proceso de Gestión de TIC, los cuales son reportados por la Oficina de Control Interno, la Subdirección General de Gestión Corporativa y la Oficina de Relacionamiento y Servicio a la Ciudadanía. Al respecto es necesario aclarar que también se reportan en el documento “Formato FO-PE-01 *Caracterización de Indicadores de Gestión y Recolección de Información*”, pero en dicho documento no son de obligatorio cumplimiento como sí lo son en el BSC.

De acuerdo con el BSC, se miden semestralmente, pero cuenta con reportes trimestrales (por los reportes trimestrales que realiza la OCI). Con corte al 30 de septiembre de 2022 se ha tenido el siguiente comportamiento:

- **Derechos de Petición respondidos con oportunidad:** El indicador, según su objetivo, pretende “Medir la oportunidad en el cumplimiento de los requisitos legales de las respuestas dadas a la ciudadanía a través del sistema Orfeo” y está relacionado con el proceso de Gestión Social y Servicio a la Ciudadanía. Se mide, según lo registrado en el campo “FUENTE DATOS”, con base en el “Reporte sistema Orfeo”. La frecuencia de medición planteada es trimestral. El cumplimiento del indicador fue del 100 % dado que la dependencia respondió oportunamente 8 de los 8 derechos de petición que le fueron asignados hasta el 30 de septiembre de 2022.

Imagen N.º 11. Gráfica del indicador “Derechos de Petición respondidos con oportunidad” de la STRT, corte 30/09/2022

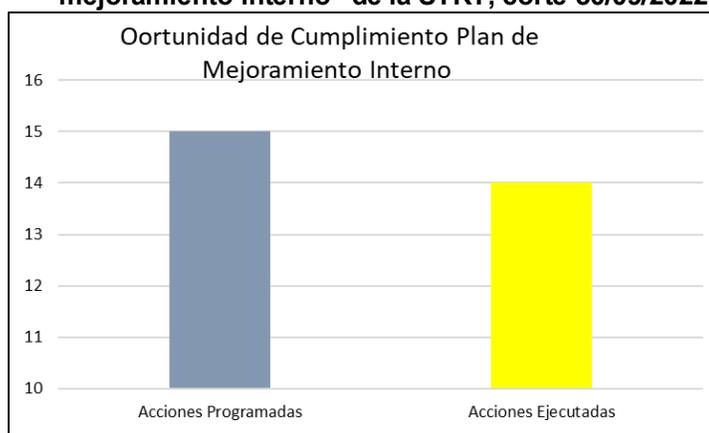


Fuente: Reporte BSC al 30/09*2022 - **Elaboración** Equipo Auditor

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

- **Porcentaje de oportunidad en cumplimiento de acciones de plan de mejoramiento interno:** El indicador, según su objetivo, busca “Medir la oportunidad del cumplimiento de acciones establecidas en el Plan de mejoramiento interno” y está relacionado con el proceso de Mejoramiento Continuo. Se mide con base en lo registrado en el “Aplicativo institucional para seguimiento a planes de mejoramiento - CHIE”. El cumplimiento del indicador fue de 93,33 % dado que la dependencia efectuó oportunamente 14 acciones de 15 que se registraron en el sistema CHIE.

Imagen N.º 12. Gráfica del indicador “% de oportunidad en cumplimiento de acciones de plan de mejoramiento interno” de la STRT, corte 30/09/2022



Fuente: Reporte BSC al 30/09/2022 – Elaboración Equipo Auditor

- **Porcentaje de oportunidad en cumplimiento de acciones de plan de mejoramiento externo:** El indicador, según su objetivo, busca “Medir la oportunidad del cumplimiento de acciones establecidas en el Plan de mejoramiento externo” y está relacionado con el proceso de Mejoramiento Continuo. Se mide con base en lo registrado en el “Aplicativo institucional para seguimiento a planes de mejoramiento - CHIE”, en relación con los planes de mejoramiento que se deriven de ejercicios de auditoría de entes de control como la Contraloría de Bogotá D. C: o la Contraloría General de la República. De acuerdo con la información reportada, se evidenció que la Subdirección Técnica de Recursos Tecnológicos no tuvo planes de mejoramiento con entes externos durante los tres primeros trimestres de 2022.
- **Avance Transformación Digital IDU:** este indicador, a cargo de la Subdirección General de Gestión Corporativa - SGGC, se encuentra asociado con el objetivo estratégico “4. Consolidar la transformación de la entidad de forma que seamos innovadores, ágiles, íntegros, transparentes y sostenibles”, presentó un avance del 80%, de acuerdo con lo programado, y se observó que las metas se cumplieron acorde con el análisis realizado en el aplicativo “al realizar la Estructuración del Proyecto con los siguientes avances: Análisis, Diseño e implementación del Gobierno de Datos en los ámbitos: gobernanza, calidad, migración, ciclo de vida y administración de los datos, Aplicación (WEB-APP) implementada como una solución integral de atención inteligente al ciudadano de manera presencial y/o virtual, para optimizar el ciclo del servicio con reportes de gestión”.
- **Avance del programa de arquitectura empresarial:** este indicador, a cargo de la SGGC, también se encuentra asociado con el objetivo estratégico “4. Consolidar la transformación de la entidad de forma que seamos innovadores, ágiles, íntegros, transparentes y sostenibles” y con el proyecto estratégico “4.1. Ajuste del diseño de la entidad de cara a facilitar la integración”. Presentó también un nivel de cumplimiento del 80%, de acuerdo con lo programado, y se observó que las metas se cumplieron acorde con el análisis realizado en el aplicativo:

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

“Definición de la estrategia para la realización del ejercicio.

Declaración del trabajo de AE.

Línea base (Arquitectura Actual).

Línea destino (Arquitectura Objetivo).

Desarrollo del trabajo de AE.

Arquitectura actual.

Análisis de Brechas.

Mapa de ruta.

Evaluación del ejercicio de AE.

Construcción y despliegue prototipos funcionales para dos (2) de los procesos priorizados y acordados con el equipo ejecutivo de articulación AE – BIM de dos (2) proyectos piloto (soluciones para asegurar las arquitecturas TOBE propuestas), convenidos con la Subdirección General de Desarrollo Urbano (SGDU)”.

La siguiente tabla refleja el cumplimiento de los indicadores de la SGGC:

Tabla N.º 11. Resultados Indicadores de la SGGC en relación con Gestión de TIC- Corte 30/06/2022

Nº	Nombre Indicador	Propósito	Tipo	Fórmula	Meta Total Programada (anual)	Programado semestre	Ejecutado semestre	% Cumplimiento o semestral	Acumulado anual
SGGC. 3	Avance Transformación Digital IDU	Medir el Porcentaje de avance en la implementación del proceso de Transformación digital (interno y Externo)	Eficacia	$(\text{SUM } \% \text{ de implementación en proyectos de transformación digital} / \text{Número de Proyectos de transformación digital}) \times 100\%$	100 %	80 %	80 %	100 %	80 %
SGGC. 4	Avance del programa de arquitectura empresarial	Medir los dominios claves del modelo de arquitectura empresarial	Eficacia	$(0,50 * \text{nivel de madurez para el cumplimiento de la política de gobierno digital (Habilitador de AE)} + 0,50 * \text{avance de la consultoría de AE}) * 100\%$	100 %	80 %	80 %	100 %	80 %
Valor acumulado						80 %	80 %	100 %	80 %

Fuente: BSC Reporte de Indicadores del IDU - Corte al 30/06/2022. Elaboración: Equipo auditor.

- Plan de Acción Estratégico del proceso

Este instrumento mide el avance en las diferentes acciones relacionadas con proyectos estratégicos del IDU, para el caso, a cargo del proceso de Gestión de Tecnologías de Información y Comunicación. Con corte al 30/06/2022, se evidenciaron siete acciones asociadas al mismo.

Con relación al cumplimiento de las acciones, para todas fue igual o superior al 100 %, clasificándolas en nivel Bueno y Distinguido. No obstante, se recomienda realizar los ajustes pertinentes, porque las metas posiblemente se encuentran subestimadas.

Ahora bien, sobre los soportes de cumplimiento de las acciones a cargo de la STRT, el proceso aportó diversas evidencias, de acuerdo con lo consignado en el archivo “PAE 2022_CONSOLIDADO”. Las observaciones del equipo auditor se presentan en la siguiente tabla, en la columna respectiva:

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Tabla N.º 12. Plan de Acción Estratégico – corte 30/06/2022

Acción	Producto/ Entregable	Meta Primer Semestre		Descripción del Avance del Primer Semestre	OBSERVACIONES DEL EQUIPO AUDITOR
		Progr amad a	Ejecut ada		
Fortalecer las capacidades de gestión de incidentes informáticos para reducir los impactos ante una interrupción inesperada de los servicios institucionales y detectar posibles alertas.	Actualización del Plan de seguridad de la información relacionadas con la gestión de incidentes, Plan de recuperación de desastres y Plan de tratamiento de riesgos del SGSI.	30%	30%	Durante el semestre la STRT ha realizado las actualizaciones de los planes, cumpliendo con la meta trazada para el periodo	Se obtuvo un 100 % de la meta al evidenciarse la actualización de los planes de seguridad de la información, Plan de recuperación de desastres y Plan de tratamiento de riesgos del SGSI.
Implementar y fortalecer el Modelo de Gobierno de Datos dando cumplimiento al lineamiento de Información y Gobierno del Dato del Mintic.	Estructuración proyecto para el Gobierno de Datos en los ámbitos: gobernanza, calidad, migración, ciclo de vida y administración de los datos.	20%	20%	Como parte de la transformación digital, el área realizó en primer semestre la estructuración inicial del Gobierno de Datos, en este sentido se solicitó incluir los anexos.	Se logró un cumplimiento del 100 % para el semestre, al comprobarse que la STRT realizó la estructuración del Gobierno de Datos.
Ejecutar el segundo ciclo del proyecto de Arquitectura Empresarial.	Plan de implementación (hoja de ruta) del Segundo ciclo del proyecto de Arquitectura Empresarial De acuerdo a Contrato IDU-1671-2021 ERNST & YOUNG.	80%	97%	Durante el primer semestre del año 2022, se desarrollaron las siguientes Fases: Fase 1. Definición de la Estrategia para de (sic) Arquitectura Empresarial del IDU: * Contextualización y alineación Estratégica * Levantamiento de información, sensibilización y alineamiento sobre visión.	La meta fue superada y logró un avance del 121,2 %, debido a que, durante el semestre, se finalizó la consultoría de Ernest & Young, empresa responsable del primer ciclo de Arquitectura Empresarial del IDU.
Articular la implementación de la metodología BIM con los lineamientos del MRAE V2 del Mintic en el segundo ciclo del proyecto de Arquitectura Empresarial.	Validación de los servicios de negocio en dos proyectos misionales piloto, definidos en la articulación de la metodología BIM con la Arquitectura Empresarial, según Contrato IDU-1671-2021, entregable E3-01-Documento del desarrollo del ejercicio de Arquitectura Empresarial ADD - Prototipo y despliegue de 2 procesos priorizados en la implementación de la metodología BIM aplicado a dos (2) proyectos misionales o de infraestructura.	80%	90%	Para el primer semestre del año 2022, se recibieron los flujogramas del proceso de CHATBOT, y se realizó la implementación por parte del proveedor. El sistema se encuentra instalado, configurado y puesto en producción.	Se logró un avance del 112,5 % Como parte del proyecto de Arquitectura Empresarial fueron realizados varios prototipos BIM, los soportes pueden consultarse en el micrositio: https://www.idu.gov.co/page/bim-en-el-idu
Coordinar la implementación de herramientas tecnológicas innovadoras para mejorar la experiencia del usuario	Chatbot personalizado e implementado según contrato CCE-82346-2021	25%	90%	Para el primer semestre del año 2022, se recibieron los flujogramas del proceso de CHATBOT, y se realizó la implementación por parte del proveedor. El sistema se encuentra instalado, configurado y puesto en producción.	Con esta acción se logró un cumplimiento del 360 %, considerando el producto que es Chatbot Fulvia el cual puede verse en operación en el portal web del IDU.
Coordinar la implementación de herramientas tecnológicas innovadoras para mejorar la experiencia del usuario	Solución de turnos digitales implementado con el contrato IDU-1626-2021	25%	98%	Para el primer semestre del año 2022, 1. Se ajustó el software de acuerdo con los requerimientos de la Oficina de Relacionamiento y Servicio a la Ciudadanía.	De acuerdo con la información suministrada, se pudo establecer que se logró un cumplimiento del 392 %. La segunda línea de defensa le <i>"solicita al área incluir soportes para facilitar el</i>

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Acción	Producto/ Entregable	Meta Primer Semestre		Descripción del Avance del Primer Semestre	OBSERVACIONES DEL EQUIPO AUDITOR
		Programada	Ejecutada		
				<p>2. Se configuraron perfiles de usuarios y usuarios en el software.</p> <p>3. Se configuraron equipos de cómputo de usuario final.</p> <p>4. Se capacitó a los 29 usuarios correspondientes a las licencias adquiridas.</p> <p>5. Se instalaron equipos y players de acuerdo a lo contratado.</p> <p>Una vez surtido todo el proceso el sistema entro en producción, y se encuentra instalado y configurado.</p>	<i>análisis, de forma concreta el plan de implementación que da cuenta del avance del proyecto</i> , por lo cual se recomienda tener en cuenta esta observación de la OAP para complementar la información de reporte de acciones de PAE.
Diseñar, desarrollar e implementar una solución tecnológica para el Fondo Compensatorio de Cesiones Públicas el cual está compuesto por "pago compensatorio de estacionamientos y pago compensatorio de obligaciones urbanísticas".	Componente tecnológico implementado para trámite de pago al Fondo Compensatorio de estacionamientos	25%	75%	<p>En la vigencia del primer semestre del año 2022, se ejecutaron las siguientes actividades:</p> <p>1. Ajuste aplicativo según solicitud del usuario líder que incluye Ajuste de estados y transiciones</p> <p>2. Ajuste modelo/vista bitácora notificación</p> <p>Ajuste de la creación de las notificaciones de acuerdo la obligatoriedad de algunos campos según el estado</p> <p>3. Ajuste modelo/vista solicitud</p> <p>Se agregan nuevos atributos asociados a la licencia y al pago según solicitud del usuario líder</p> <p>4. Creación modelo/vista reingreso para permitir los reingresos de las solicitudes devueltas a las curadurías.</p>	<p>Esta acción se cumplió al 300 % al superar la meta. La descripción del avance es coherente con el producto de la acción.</p> <p>La segunda línea de defensa le solicita al área "<i>incluir soportes para facilitar el análisis</i>", por lo cual se recomienda tener en cuenta esta observación de la OAP para complementar la información de reporte de acciones de PAE.</p>

Fuente: PAE publicado en la página WEB IDU **Elaboración:** Propia del equipo auditor.

Con base en lo presentado en la tabla anterior, con corte al 30/06/2022, se puede observar, según se especifica en el capítulo 3, numeral 6, del Documento "Indicadores de Gestión en la Práctica" Versión 7 - DU PE 17, un cumplimiento "Distinguido" de las acciones incluidas en el PAE, toda vez que en promedio alcanzó 212,24 %, teniendo en cuenta que dos de las acciones presentan un avance del 100 % y cinco superaron la meta planteada.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

3. Informe de seguimiento a las acciones de mejora en curso a cargo del proceso

Una vez revisada la base de datos en el aplicativo CHIE: Plan Mejoramiento Institucional, se encontraron formuladas acciones de planes de mejoramiento interno, relacionadas con las actividades críticas de la caracterización del proceso, pendientes por evaluar efectividad.

Tabla N.º 13. Evaluación de efectividad de acciones de planes de mejoramiento

Acción	Hallazgo	Acción Propuesta	Evaluación de Efectividad
2514	No Conformidad N° 1. Acciones de planes de mejoramiento inefectivas - Gestión de TIC.	Incluir en la EDL para funcionarios un compromiso relacionado con la gestión oportuna de acciones de mejoramiento y lo propio para contratistas PSP, mediante la creación de un factor de evaluación asociado al informe mensual de actividades.	<p>De conformidad con lo revisado en el aplicativo CHIE, se pudo establecer que la acción se encuentra en estado terminado, razón por la cual se procedió a evaluar los anexos que sustentan el avance de la acción encontrándose lo siguiente: se revisaron dos informes de actividades de algunos contratistas de la dependencia y se evidencia que se incluyeron los compromisos en el desarrollo de los contratos.</p> <p>De igual manera, se evidenció que en la dependencia se ha realizado seguimiento a tres funcionarios con relación a la gestión oportuna de las acciones de mejoramiento a cargo. Adicionalmente, se evidenció que realizaron dos presentaciones para toda la dependencia, en las cuales uno de puntos desarrollados consistió en enfatizar la obligación de cumplir con las acciones de mejoramiento a cargo. También se observó la modificación de la evaluación del desempeño para los casos que aplican.</p> <p>No obstante, se considera que el tiempo transcurrido entre la calificación de esta acción (04/08/2022) y la fecha de este informe no ha sido suficiente para dar un concepto objetivo de efectividad de la acción. Por tanto, la evaluación de efectividad se posterga para un ejercicio posterior de auditoría o seguimiento específico.</p>
2515		Monitorear el cumplimiento del Compromiso Labora (planta) / factor de evaluación (PSP) en relación con la gestión de acciones de mejoramiento asignadas	<p>Una vez consultado el desarrollo de la acción en el aplicativo CHIE: Plan Mejoramiento Institucional, se evidenció que se encuentra en estado terminado, razón por la cual se procedió a evaluar los anexos que sustentan el avance de la acción encontrándose lo siguiente: Se evidenció la inclusión de la cláusula relacionada con la gestión de acciones de mejoramiento asignadas en todos los contratos de la dependencia; de igual manera, se revisaron dos informes de actividades mensuales del contrato IDU-475-2022 y se observó que se relacionan los avances de las acciones a cargo del contratista.</p> <p>Así mismo, se verificó que para el caso del personal de planta se diligenció una planilla como mecanismo de control para verificar las tareas relacionadas con las acciones de mejoramiento a cargo. Finalmente, se evidenció que, con acta de reunión del 16/05/2022, se impartieron instrucciones con respecto al tema de planes de mejoramiento a cargo.</p> <p>No obstante, se considera que el tiempo transcurrido entre la calificación de esta acción (04/08/2022) y la fecha de este informe no ha sido suficiente para dar un concepto objetivo de efectividad de la acción. Por tanto, la evaluación de efectividad se posterga para un ejercicio posterior de auditoría o seguimiento específico.</p>
2518	No Conformidad N° 3. Debilidades en el reporte de materialización de riesgos de gestión del proceso Gestión de TIC.	Revisar las matrices de riesgos del proceso por un par (chequeo cruzado), que valide la información reportada	Se revisaron los documentos aportados en CHIE como evidencia del cumplimiento de la acción y se verificó que, de acuerdo con el reporte del auditor, esta acción fue terminada. Teniendo en cuenta que, de acuerdo con los reportes de la dependencia, no se han presentado eventos de materialización de riesgos de gestión o de corrupción, se posterga el análisis de efectividad para un ejercicio posterior de auditoría o seguimiento específico.
2520	No Conformidad N° 4. Desactualización de activos de información del proceso de Gestión de Tecnologías de	Asignar la responsabilidad operativa de solicitar la actualización del inventario de activos de información, al enlace del SGSI en la SGGC	Se solicitó el listado de activos de información del proceso de Gestión de Tecnologías de Información y Comunicación. Se revisó la información con base en la Circular 85 de 2020 de propiedad de los sistemas de información y no se evidenció ningún faltante de los sistemas a cargo del proceso. El proceso manifestó que "La fecha más reciente de actualización de los activos de información del proceso Gestión de TIC corresponde al usuario Wilser Hanney

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Acción	Hallazgo	Acción Propuesta	Evaluación de Efectividad
	Información y Comunicación.		<p><i>Palacios Sanchez con fecha 28/10/2022</i>". Se verificó que el usuario tenía el inventario es estado "Visto bueno". Este estado significa que hace falta la aprobación del oficial de seguridad y, posterior a esta, la del líder del proceso.</p> <p>Dado que es solo un registro y ya se efectuó la actualización, quedando pendientes dos aprobaciones, esta acción se considera efectiva y se recomienda el cierre.</p> <p>Al proceso se le sugiere efectuar las aprobaciones faltantes respecto de los activos de información del usuario mencionado.</p>
2521	No Conformidad N° 1. Acciones de planes de mejoramiento inefectivas - Gestión de TIC.	Monitorear con periodicidad mensual los estados de los casos registrados en el sistema Aranda	<p>Esta acción terminó el 30/06/2022 y se calificó como cumplida en el seguimiento a planes de mejoramiento, efectuado a inicios de julio de 2022. Para el análisis de efectividad se solicitó un listado de información de casos registrados para atención en mesa de ayuda en agosto de 2022. En la información entregada, un archivo con 5.531 registros, se pudo evidenciar que la mayor cantidad de casos (99,9 %) se encontraba cerrada, así: 5.046 fueron cerrados en agosto de 2022, es decir, el mismo mes de registro, 396 fueron cerrados en septiembre, 74 en octubre y 14 en noviembre de dicho año. Esto significa que la acción de mejora 2521 cumplió su objetivo de "Realizar control al ciclo de vida de casos registrados en el sistema Aranda", por tanto, se considera efectiva y se recomienda su cierre en el aplicativo institucional de planes de mejoramiento.</p>
2522		Revisar la documentación del mapa de procesos del proceso Tecnologías de Información y comunicación, ajustado al plan de acción de la OAP	<p>Dentro del desarrollo de la auditoría se revisaron diversos documentos del proceso y se encontraron diversas situaciones como:</p> <ul style="list-style-type: none"> Los términos y definiciones de los siguientes documentos no se encuentran publicados en el Glosario de términos del IDU: IN-TI-02 Instructivo Solicitud de Soporte Técnico por Agenda USDK, IN-TI-06 Uso Adecuado de los Recursos TI. IN-TI-07 Administración del Directorio Activo DU-TI-01 Catálogo de Servicios de Tecnologías de la Información DU-TI-06 Políticas Operacionales de Tecnologías de Información y Comunicación. MG-TI-016 Manual Backups y Recuperación de la Información MG-TI-18 Políticas de Seguridad de la Información. PR-TI-02 Gestión de Usuarios TI IDU PR-TI-11 Generación de Copias de Seguridad PR-TI-16 Gestión de la Capacidad Se encontró incongruencia en relación con la periodicidad de revisión de los derechos de acceso a los recursos de TI que está señalada en el instructivo IN-TI-16 "Revisión de los Derechos de Acceso a los Recursos de TI", versión 2, que dice "Durante cada vigencia"; el numeral 6.3.5.4 "Revisión de los derechos de acceso de usuarios" del manual operativo MG-TI-18 "Políticas de Seguridad de la Información", versión 5, que señala "mínimo trimestralmente" y el control 4 del riesgo de corrupción C.TI.01, que indica "de manera bimestral". El procedimiento PR-TI-12 "Restauración de Copias de Seguridad", versión 1, en su numeral 1.1.3 "Marco Normativo" refiere la "Resolución interna 447 de 2012 "Por la cual se reglamenta el Sistema Integrado de Gestión, se reorganiza su Sistema de Coordinación Interna y se crean los equipos institucionales", la cual está derogada. El procedimiento PR-TI-02 está incompleto toda vez que no refiere ninguna actividad relacionada con "[...] las modificaciones y mantenimiento de dichas credenciales hasta la realización del proceso de desvinculación que inactiva y cancela dichos privilegios de acceso lógico de los funcionarios". En la política operacional 5 del procedimiento PR-TI-16 está referida la actividad "1.1.6.2 identificarla (sic) capacidad actual", la cual no existe en el citado procedimiento, porque el numeral correcto es "1.6.2. Identificar la capacidad actual". El marco normativo del procedimiento PR-TI- refiere la Norma Técnica NTC GP-1.000, Calidad en la gestión pública, ya derogada. Adicionalmente habla del PETIC, pero la denominación actual es PETI, para referirse al documento que corresponde al Plan Estratégico de Tecnologías de la Información.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Acción	Hallazgo	Acción Propuesta	Evaluación de Efectividad
			<ul style="list-style-type: none"> El manual MG-TI-18 "Políticas de Seguridad de la Información", en el numeral 6.3.16.1 "Copias de Respaldo de Información Centralizada", refiere al procedimiento PR-TI-17 "Gestión de Servidores", numeral 4.1.1.4 7 "Programar copia de respaldo total de servidor de aplicaciones", que no corresponde con el procedimiento vigente. <p>Las situaciones enunciadas dan lugar a la cancelación de la acción por considerarse inefectiva, por lo cual se recomienda su cancelación.</p>
2523		Diligenciar el formato FO-TI-30 de manera automatizada, mediante la creación de un componente tecnológico, que tome la información de capacidad del SIEM	<p>Esta acción terminó el 31/12/2021 y se calificó como cumplida en el seguimiento a planes de mejoramiento, efectuado a inicios de enero de 2022, dado que fue elaborado un <i>script</i> que permitía, a la STRT, tomar los datos del SIEM y consignarlos automáticamente en el formato FO-TI-30 "Control de la capacidad".</p> <p>No obstante, en la revisión del tema de la gestión de la capacidad efectuada en la presente auditoría se evidenció que esa automatización no se utilizó y si bien hubo medición de la capacidad, ésta se efectuó manualmente. Sólo hasta septiembre de 2022 se retomó la automatización y efectuaron mediciones con un <i>script</i> modificado para un piloto de cambio de la presentación de la información en le FO-TI-30.</p> <p>Por tanto, la acción se considera inefectiva.</p>
2578	Norma ISO/IEC 27001:2013, anexo A, control A.12.3 Copias de respaldo	Modificar el Manual de Copias de Seguridad MG-TI-16 para incluir una política de planeación y ejecución de pruebas de restauración de backups	<p>Estas acciones surgieron a raíz de la auditoría de seguimiento a la certificación del SGSI, realizada en 2021, por el ente certificador Bureau Veritas.</p> <p>Ahora bien, el numeral 7.6.7 "Informe de Seguimiento al Plan" del procedimiento "Formulación, monitoreo y seguimiento a planes de mejoramiento", PR-MC-01, indica, en el acápite de Observaciones de este numeral, que "[...]. Para las acciones derivadas de auditorías externas, pese a que la Oficina de Control Interno realizará el seguimiento de las mismas, el cierre efectivo de la acción y/o su evaluación de efectividad, está supeditado al dictamen de la entidad certificadora."</p>
2579		Elaborar una restauración de prueba a un objeto definido aleatoriamente	<p>Por tanto, la evaluación de su efectividad debió realizarla el ente certificador SGS, que fue el que realizó la auditoría de seguimiento a la certificación en 2022. Sin embargo, la OCI, a la fecha, no ha recibido el informe respectivo.</p> <p>En razón de lo anterior, no se recomienda su cierre o cancelación en la presente auditoría y se efectuarán las acciones pertinentes una vez la STRT y/o la Oficina Asesora de Planeación (OAP) remitan a la OCI el informe elaborado por SGS.</p>
2580	Norma ISO/IEC 27001:2013, Anexo A, control 12.1.2 Gestión de Cambios	Realizar una sesión de sensibilización sobre el uso del sistema Aranda (módulo cambios)	
2581		Realizar dos sesiones de sensibilización sobre el procedimiento PR-TI-08	
2582		Revisar y actualizar el procedimiento PR-TI-08	
2583		Cerrar los cambios del año 2021 que estén abiertos	

Fuente: Aplicativo CHÍE de Planes de Mejoramiento – listado de acciones con corte 31/10/2022. **Evaluación:** Equipo auditor.

En resumen, de las acciones citadas en la tabla precedente, 2 se consideraron efectivas (2520 y 2521), por tanto, se sugiere su cierre y 2 se consideraron inefectivas (2522 y 2523), por tanto, se sugiere su cancelación. En cuanto a las acciones 2514 y 2515 y 2518, según lo descrito en la tabla, deberán evaluarse en otros ejercicios de auditoría o seguimiento. La evaluación de efectividad de las 6 acciones restantes (2578, 2579, 2580, 2581, 2582 y 2583) depende del concepto que haya la entidad que realice la auditoría de seguimiento a la certificación del Subsistema de Seguridad de la Información (SGSI).

Para cada una de las acciones inefectivas, el proceso deberá formular una o más acciones diferentes que permitan eliminar la(s) causa(s) de los hallazgos o no conformidades inicialmente detectados.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

4. Informe de seguimiento a riesgos del proceso

Este informe está planteado, en la caracterización del proceso, como un producto. En entrevista con el personal del proceso se determinó que dicho informe se refiere a la remisión de la información de monitoreos y/o seguimientos de los riesgos del proceso a las dependencias que corresponda en los tiempos establecidos por ellas.

Así, para la vigencia 2022, de acuerdo con los reportes aportados por la OAP y la SGGC, que son las dependencias encargadas de administrar el sistema de riesgos de la Entidad, se evidenció que la STRT realizó las actualizaciones de la matriz de riesgos del proceso en las dos oportunidades establecidas por el Instituto y dentro de los plazos establecidos.

De acuerdo con el reporte, se verificó que con los memorandos 20225360169993 (11/05/2022) y 20225360316533 (08/09/2022), fueron reportadas oficialmente las actualizaciones de las matrices de riesgo de gestión y corrupción correspondientes al primer y segundo cuatrimestres de la vigencia 2022.

Revisado el ORFEO, se pudo establecer que con radicados 20225360213933 (13/06/2022) y 20225360323753 (15/09/2022), la STRT reportó ante la SGGC las matrices de riesgos de soborno de los dos primeros cuatrimestres del año.

De acuerdo con la documentación y el reporte de la STRT, en esta vigencia no se han materializado los riesgos identificados y se ha cumplido con los reportes establecidos.

5. Informe de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS

Se solicitó al proceso este informe y allegó el archivo “*Informe_junio2022.pdf*” que presenta un documento titulado “*INFORME EJECUCIÓN STRT-MESA DE SERVICIOS MES DE JUNIO DE 2022*”. Señala el informe que, en junio de 2022, se registraron 3.921 casos y muestra unas gráficas de cantidades de casos registrados por autor, atendidos por especialista, registrados y atendidos por autor y especialista, por categoría y estado de casos.

Sin embargo, no se observó análisis frente a los ANS establecidos en el catálogo de servicios de TI, DU-TI-01. En el numeral “6. ESTADO DE CASOS” del precitado informe, refiere el archivo de Excel “*TiemposAtencionmesJunio2022.xlsx*”. Éste contiene los nombres de 9 personas, que eran agentes de mesa de ayuda en junio, con unas fechas (como se ve en la imagen N.º 13), pero tampoco presenta un análisis de tendencias de cumplimiento de los acuerdos de nivel de servicio.

Por lo anterior se generó un hallazgo de auditoría.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Imagen N.º 13. Recorte que muestra parte del contenido del archivo “*TiemposAtencionmesJUnio2022.xlsx*”

Etiquetas de fila	
<ul style="list-style-type: none"> ▣ Cesar Augusto Tiga Fonseca <ul style="list-style-type: none"> ▣ 21/06/2022 15:35 <ul style="list-style-type: none"> 21/06/2022 16:33 ▣ 22/06/2022 17:47 <ul style="list-style-type: none"> 22/06/2022 18:24 ▣ 23/06/2022 13:50 <ul style="list-style-type: none"> 23/06/2022 15:53 ▣ 23/06/2022 13:53 <ul style="list-style-type: none"> 23/06/2022 15:43 ▣ 23/06/2022 16:09 <ul style="list-style-type: none"> 23/06/2022 19:37 ▣ 23/06/2022 19:24 <ul style="list-style-type: none"> 23/06/2022 19:25 ▣ 25/06/2022 18:37 <ul style="list-style-type: none"> 25/06/2022 18:53 ▣ 29/06/2022 18:11 <ul style="list-style-type: none"> 29/06/2022 18:46 ▣ Cindy Johanna Ramirez Meza <ul style="list-style-type: none"> ▣ 21/06/2022 9:08 <ul style="list-style-type: none"> 22/06/2022 14:14 ▣ 21/06/2022 9:36 <ul style="list-style-type: none"> 21/06/2022 11:35 ▣ 21/06/2022 9:55 <ul style="list-style-type: none"> 21/06/2022 11:32 ▣ 21/06/2022 10:15 <ul style="list-style-type: none"> 21/06/2022 12:58 ▣ 21/06/2022 10:20 <ul style="list-style-type: none"> 21/06/2022 10:26 	<ul style="list-style-type: none"> ▣ Marlon Anderson Casallas Contreras <ul style="list-style-type: none"> ▣ 21/06/2022 9:19 <ul style="list-style-type: none"> 21/06/2022 9:23 ▣ 21/06/2022 13:59 <ul style="list-style-type: none"> 21/06/2022 15:14 ▣ 22/06/2022 13:02 <ul style="list-style-type: none"> 22/06/2022 15:59 ▣ 22/06/2022 15:52 <ul style="list-style-type: none"> 22/06/2022 15:59 ▣ 23/06/2022 12:11 <ul style="list-style-type: none"> 23/06/2022 15:04 ▣ 23/06/2022 12:11 <ul style="list-style-type: none"> 24/06/2022 12:34 ▣ 23/06/2022 12:12 <ul style="list-style-type: none"> 23/06/2022 14:54 ▣ 23/06/2022 12:18 <ul style="list-style-type: none"> 23/06/2022 14:57 ▣ 24/06/2022 12:35 <ul style="list-style-type: none"> 24/06/2022 12:36 ▣ 24/06/2022 17:13 <ul style="list-style-type: none"> 24/06/2022 17:20 ▣ Ruben Dario Gomez Avila <ul style="list-style-type: none"> ▣ 21/06/2022 9:08 <ul style="list-style-type: none"> 21/06/2022 9:09 ▣ 21/06/2022 9:10 <ul style="list-style-type: none"> 21/06/2022 16:38 ▣ 21/06/2022 9:53 <ul style="list-style-type: none"> 21/06/2022 9:54

Fuente: STRT. Elaboración: Propia del equipo auditor.

No se observan conclusiones ni análisis de situaciones que pueden afectar o mejorar la prestación del servicio, para la toma de acciones.

ANÁLISIS DE LA RESPUESTA DE LA STRT AL INFORME PRELIMINAR DE AUDITORÍA

El informe preliminar de auditoría al proceso de Gestión de Tecnologías de Información y Comunicación fue comunicado, a la SGGC, la DTAF y la STRT, mediante correo electrónico del 21/12/2022 y socializado en reunión de cierre del mismo día. Se recibió respuesta de la STRT, mediante correo electrónico del 23/12/2022.

A continuación, se presentan los argumentos de la STRT y el análisis de respuesta realizado por el equipo auditor:

Frente al hallazgo N.º 2 “Incumplimiento de algunas actividades relacionadas con la gestión de copias de seguridad”, la STRT señaló lo siguiente:

“Se solicita de manera respetuosa validar este hallazgo teniendo en cuenta que diariamente la Subdirectora Técnica de Recursos Tecnológicos recibe por correo electrónico un informe sobre el estado de backups y restauraciones realizadas (cuando aplica), se adjunta pantallazo y documento de evidencia “Informe de seguimiento - Monitoreo IDU - BACKUP - Noche- 21 - Diciembre 2022”.”

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

Fwd: TLP:ROJO - Reporte diario IDU-Backup 21/12/2022 - STS Recibidos x

A Arleth Patricia Saurith Contreras 11:37 (hace 1 hora)

para mí ▾

----- Forwarded message -----
 De: Mesa de Servicios STS <soporte@stssa.com.co>
 Date: jue, 22 dic 2022 a las(s) 00:18
 Subject: TLP:ROJO Reporte diario IDU Backup 21/12/2022 STS
 To: Arleth Patricia Saurith Contreras <arleth.saurith@idu.gov.co>, Lucero Quastar@idu.gov.co <lucero.quastar@idu.gov.co>, Erwing Javier Gomez Mendez <erwing.gomez@idu.gov.co>
 Cc: Maria Marilyn Lucero Reyes Palomino <maria.reyes@holistica-it.com.co>

Cordial Saludo,

Ingenieros Con el fin de dar cumplimiento al requerimiento de la ficha técnica – 3. ÍTEM. RENOVACIÓN Y CRECIMIENTO A LA SOLUCIÓN ALMACENAMIENTO CENTRALIZADO - RESPALDO A DISCO numeral 3.12. Soporte Telefónico y Monitoreo - CONTRATO DE COMPRAVENTA NÚMERO 514 DE 2022. CELEBRADO ENTRE EL INSTITUTO DE DESARROLLO URBANO Y UNION TEMPORAL BACKUP IT 2022, se adjunta el reporte diario de monitoreo de la plataforma de Backup

Cordialmente,

Re: TLP:ROJO - Reporte diario IDU-Backup 22/11/2022 - STS Usuarios externos Recibidos x

A Arleth Patricia Saurith Contreras 11:38 (hace 2 horas)

para Mesa, mí ▾

El mié, 23 nov 2022 a las(s) 00:21, Mesa de Servicios STS (soporte@stssa.com.co) escribió:

Cordial Saludo,

Ingenieros Con el fin de dar cumplimiento al requerimiento de la ficha técnica – 3. ÍTEM. RENOVACIÓN Y CRECIMIENTO A LA SOLUCIÓN ALMACENAMIENTO CENTRALIZADO - RESPALDO A DISCO numeral 3.12. Soporte Telefónico y Monitoreo - CONTRATO DE COMPRAVENTA NÚMERO 514 DE 2022. CELEBRADO ENTRE EL INSTITUTO DE DESARROLLO URBANO Y UNION TEMPORAL BACKUP IT 2022, se adjunta el reporte diario de monitoreo de la plataforma de Backup

Cordialmente,



Centro de atención y servicios en tecnologías de información
CAST

MESA DE SERVICIOS STS

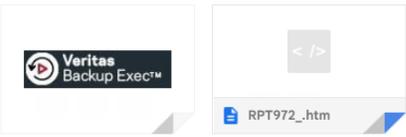
Alerta de Backup Exec: Trabajo satisfactorio (Servidor: "BK03CC01") (Trabajo: "Informe Restauraciones Diarias") Recibidos x

I Veritas <veritas@idu.gov.co> 12:26 (hace 1 hora)

para mí ▾

(Servidor: "BK03CC01") (Trabajo: "Informe Restauraciones Diarias") Completada satisfactoriamente.

2 archivos adjuntos • Analizado por Gmail



FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Análisis del equipo auditor:

El hallazgo consta de 3 ítems o aspectos relacionados con copias de seguridad a saber:

- La presentación a la subdirectora de la STRT, de forma bimestral, de informes del estado de los trabajos de generación y restauración de copias de seguridad por parte del designado para realizar la operación de copias de seguridad.
- La elaboración del plan de pruebas y la realización de pruebas periódicas aleatorias.
- El tiempo mínimo de retención, en el equipo DR6000, de los *jobs* de copias de seguridad “S3-MAR-BODEGA_ORFEO_2013” y “D1-BK03CC01_DB_BKEXEC”.

En su respuesta, la STRT refirió que la subdirectora de la STRT diariamente recibe, a través de correo electrónico, “[...] un informe sobre el estado de backups y restauraciones realizadas (cuando aplica)”. Allegó 3 imágenes que muestran 3 correos electrónicos, dos de ellos remitidos, el 23/11/2022 y el 22/12/2022, desde el correo Mesa de Servicios STS (soporte@stssa.com.co) con los asuntos “TLP:ROJO - Reporte diario IDU-Backup 22/11/2022 - STS” y “TLP:ROJO - Reporte diario IDU-Backup 21/12/2022 - STS”, respectivamente.

El tercer correo muestra una alerta de un trabajo satisfactorio, enviada por la plataforma Veritas Backup Exec, utilizada por la STRT para el control de los trabajos de copias de seguridad, aunque no es posible determinar cuándo fue enviada, ni a quién. Según el asunto, la alerta es de un trabajo llamado “Informe Restauraciones Diarias”.

Adicionalmente, fue allegado el archivo llamado “Informe de seguimiento - Monitoreo IDU - BACKUP - Noche-21 - Diciembre 2022.pdf” que contiene un “REPORTE – MONITOREO DE PLATAFORMA BACKUPS IDU” de diciembre 21 de 2022 desde las 11:59:59 hasta las 23:59:59 del mismo día.

Este último informe corresponde, según se lee en la imagen de los correos, a uno de los reportes diarios remitidos por el contratista en el marco del contrato de compraventa IDU-514-2022, celebrado entre el IDU y la Unión Temporal BACKUP IT 2022, para “[...] dar cumplimiento al requerimiento de la ficha técnica – 3. ÍTEM: RENOVACIÓN Y CRECIMIENTO A LA SOLUCIÓN ALMACENAMIENTO CENTRALIZADO –RESPALDO A DISCO numeral 3.12. Soporte Telefónico y Monitoreo [...]”.

Es decir, esos informes no son presentados por quien está designado, en la STRT, para ejecutar las actividades de operación de copias de seguridad, ni tampoco bimestralmente, según lo indica el numeral 6.2 “Operador de Copias de Seguridad y Base de Datos” del Manual *Backups* y Recuperación de la Información, código MG-TI-016, versión 6.

Además, se determinó, mediante consulta en el aplicativo SIAC, que el contrato IDU-514-2022, cuyo objeto es la “Renovación del soporte y garantías de la solución de Backup que respalda el proceso de copias de seguridad y adquisición de una plataforma complementaria de Backup para el Instituto de Desarrollo Urbano”, está en estado “TERMINADO”, dado que tenía un plazo de ejecución de 8 meses desde la suscripción del acta de inicio, lo cual sucedió el 07/04/2022. Esto significa que la fecha de terminación del contrato fue el 06/12/2022.

Por lo descrito, los informes mencionados no pueden tomarse como el cumplimiento de la actividad que debe efectuar el operador de copias de seguridad. Además, una vez terminado el contrato, no hay garantía de que los informes se sigan remitiendo a la STRT. Por tanto, se mantiene este ítem en el hallazgo.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

En relación con el plan de pruebas de copias de seguridad, en la entrevista efectuada el 22/11/2022, quien hace las veces de operador de copias de seguridad y administrador del centro de cómputo informó que no existe dicho plan⁷. Los soportes de las restauraciones evidenciadas en la ejecución de la auditoría, no obedecen a un plan de pruebas, ni se pueden considerar periódicas y aleatorias, dado que han sido originadas en solicitudes específicas. Cabe anotar que, sobre este ítem de plan de pruebas, no se realizó pronunciamiento por parte de la STRT en la respuesta al informe preliminar.

Por último, frente al tiempo de retención no hubo pronunciamiento de la STRT en la respuesta al informe preliminar de auditoría. Dado lo descrito, el hallazgo se mantiene sin modificaciones.

Frente al hallazgo N.º 4 “*Usuarios de red activos de 4 exfuncionarios de la Entidad*”, la STRT argumentó lo siguiente:

“Se solicita de manera respetuosa validar este hallazgo teniendo en cuenta que Carlos Eduardo Lamprea Robles se encuentra activo porque el área al cual pertenecía no efectuó dicha solicitud, la STRT siempre procede a través de las solicitudes de los dueños de la información, caso particular deshabilitar un usuario.

Sobre los otros usuarios, se encuentran activos por solicitudes particulares de las áreas que realizan por correo electrónico, se adjunta pantallazos.”

Fwd: Solicitud de habilitación Usuario - Jaime Anaya Blanquicett Q.E.P.D. Recibidos x Gestionados x 🔍 🖨 🔗

 **Arleth Patricia Saurith Contreras** <arleth.saurith@idu.gov.co> mar, 1 nov, 15:37 ★ ↶ ⋮
 para mí, Esperanza ▼
 por favor atender

----- Forwarded message -----
 De: **Cesar Dimas Padilla Santacruz** <cesar.padilla@idu.gov.co>
 Date: mar, 1 nov 2022 a la(s) 15:18
 Subject: Re: Solicitud de habilitación Usuario - Jaime Anaya Blanquicett Q.E.P.D.
 To: Arleth Patricia Saurith Contreras <arleth.saurith@idu.gov.co>
 Cc: Helpdesk IDU <helpdesk@idu.gov.co>, Emilia Patricia Cruz Ospina <emilia.cruz@idu.gov.co>

Estimada Arleth,
 La solicitud de mantener habilitado el correo y usuarios de Jaime se requiere por unos días, mientras reasignamos algunos asuntos que el está manejando e información que se gestionaba a través de su correo, como facturación, mensajes de Colombia Compra Eficiente de los procesos de contratación en curso, entre otros.
 La idea es que Emilia Patricia Cruz sea quien gestione los temas que hayan llegado a su buzón y redireccionar los que lleguen en este corto período.
 Igualmente, solicitar un full backup de toda su información y correos
 Les agradezco de antemano el apoyo u orientación de la mejor formas de contar con la información y poder gestionar todo lo pendiente.

César Dimas Padilla Santacruz
 Subdirector Técnico
 Subdirección Técnica de Recursos Físicos
 Instituto de Desarrollo Urbano - IDU

Análisis del equipo auditor:

La evidencia aportada por la STRT hace referencia únicamente al caso del exfuncionario fallecido, identificado con cédula 79XXX807 y presenta un correo del 01/11/2022 del Subdirector Técnico de Recursos Físicos, a la STRT, solicitando “[...] *mantener habilitado el correo y usuarios [...] por unos días [...]*”, mientras reasignaban asuntos que él manejaba. En este sentido, y con el argumento presentado, se excluye este caso de la descripción del hallazgo; sin embargo, es necesario tener presente que esta

⁷ Desde la 01 hora y 39 minutos de la grabación, se trata este tema.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

excepción no puede mantenerse indefinidamente y al momento de presentación del informe preliminar ya habían pasado más de 30 días hábiles estando el usuario activo, desde la fecha de reporte del fallecimiento.

En relación con el caso del funcionario identificado con cédula 19XXX876, en efecto, no se encontró la solicitud de la Subdirección Técnica de Recursos Físicos en el aplicativo Gestión TIC. En este sentido, se excluye este caso de la descripción del hallazgo.

Para los casos de los exfuncionarios identificados con cédula 13XXX445 y 52XXX219 sí había solicitud en Gestión TIC por parte de las áreas, por lo cual, la responsabilidad es de la STRT. Cabe anotar que, para estos 2 casos, no hubo pronunciamiento por parte de dicha dependencia.

Por lo anterior, se mantiene el hallazgo, excluyendo del mismo, los 2 casos relacionados anteriormente y en su lugar, se genera la siguiente recomendación: Realizar seguimiento a los 2 casos señalados en el informe, atinente a los usuarios identificados con cédula de ciudadanía 79XXX807 y 19XXX876, a fin de tomar las acciones pertinentes para finalizar los permisos de usuario.

Frente al hallazgo N.º 5 “Falta de análisis de tendencias de cumplimiento en el producto “6. Informe de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS””, la STRT, en la respuesta al informe preliminar argumentó lo siguiente:

“Se solicita de manera respetuosa validar este hallazgo teniendo en cuenta que si se realiza el análisis de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS en las reuniones de comité estratégico que efectúa la Subdirectora Técnica de Recursos Tecnológicos con los líderes (sic) de los equipos del área, se adjunta documento de evidencia “acta de comité estratégico”.”

Análisis del equipo auditor:

La respuesta de la STRT indica que el análisis de tendencias de cumplimiento de los ANS se efectúa en las reuniones de comité estratégico que realizan en la dependencia; no obstante, en el correo inicial de respuesta del 23/12/2022 no fue allegada la evidencia de ello. Posteriormente, en dos correos de alcance remitidos al equipo auditor el 28/12/2022, la STRT allegó otros archivos, así:

Un archivo llamado “FO-PE-14_ACTA_DE_REUNION_5 - 22082022 (1).pdf” que refleja un acta de un comité estratégico de la STRT, realizado el 22/08/2022, en cuyo desarrollo, entre otros aspectos tratados, está consignado lo siguiente:

“IV. Se realiza el análisis del catálogo de servicio para el cumplimiento de los Acuerdos de Niveles de Servicio mediante la presentación del Catálogo de Servicio.”

También adjuntaron una presentación en la que se observa una diapositiva titulada “Catalogo Virtual”, la cual sólo muestra un texto de dos numerales o temas, así: “1. Catalogo (sic) de servicio IDU – Excel” y “2. DUT101 CATALOGO DE SERVICIOS DE TECNOLOGIAS (sic) DE LA INFORMACION (sic) Y LA COMUNICACIÓN”.

Adicionalmente, allegaron el archivo de Excel “Catalogo de Servicios IDU.xls” que contiene 2 hojas, así: “CatalogoServiciosActual” relaciona 12 servicios con los tiempos de ANS manejados actualmente y

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

“PropuestaCatalogoServiciosIDU” presenta 16 servicios con los tiempos que se manejarían según la propuesta.

No obstante, en los soportes suministrados por la STRT no se observa un análisis de tendencias de cumplimiento de los ANS actuales. Por tanto, no se retira el hallazgo del informe final de auditoría.

Frente a los demás componentes del Informe, no hubo ningún pronunciamiento.

Fortalezas identificadas

- El desarrollo de herramientas para mejorar la gestión del proceso como es la implementación del software de monitoreo Zabbix, que ha permitido anticiparse a posibles caída de servicios y el piloto para optimizar la recolección de datos en el FO-TI-30 Interés del proceso de Gestión de TIC.
- El fortalecimiento e innovación en capacitaciones sobre temas del resorte del proceso, como la realización de las charlas institucionales “Hablemos de Seguridad sin Tapujos”, las cuales realiza la dependencia bimestralmente con una participación promedio de 250 servidores IDU.
- La implementación de proyectos de envergadura como el de arquitectura empresarial, que contribuyen a incrementar la robustez de la infraestructura de TI de la entidad.
- El cumplimiento de las metas establecidas para los indicadores registrados en el PAE y en el *Balanced Scorecard*.

3.1 REQUISITOS CON INCUMPLIMIENTO

Nº	Criterio	Descripción
H1	<p>PR-TI-16 GESTIÓN DE LA CAPACIDAD, v 3.</p> <p>1.5. POLÍTICA OPERACIONAL.</p> <p>“[...] 3. Se debe revisar y actualizar los valores de capacidad de cada uno de los elementos o activos de información más relevantes de los servicios prestados <u>cada tres meses</u>”. (Subrayado fuera de texto).</p> <p>1.6.15. 3 meses</p> <p>“Al inicio de cada ciclo mensual (sic) (antes de los cinco {5} primeros días hábiles) se deberá realizar la siguiente actividad”. [1.6.16. Realizar mediciones periódicas]</p> <p>Riesgo G.TI.02 Insuficiente asignación de recursos para el cumplimiento de los objetivos o actividades requeridas por el proceso</p>	<p>Hallazgo 1. Extemporaneidad en la revisión y actualización de valores de la capacidad de algunos elementos de TI (servidores de bases de datos, servidores de aplicaciones, servidores de almacenamiento, entre otros).</p> <p>Se evidenció extemporaneidad en la revisión y actualización de valores de la capacidad de elementos relevantes de TI (servidores de bases de datos, servidores de aplicaciones, servidores de almacenamiento, entre otros) que debió efectuar la STRT en 2022, dado que las mediciones no se efectuaron trimestralmente antes de los 5 primeros días hábiles de cada periodo, lo cual contraviene el numeral 3 de la política operacional y el numeral 1.6.15 del procedimiento PR-TI-16 y lo establecido en el control 1 del riesgo de gestión del proceso G.TI.02, lo cual podría afectar la toma oportuna de decisiones sobre los recursos de TI al no tener las cifras de capacidad según los tiempos establecidos y podría disminuir el control que sobre los recursos de procesamiento, almacenamiento y redes de</p>

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Nº	Criterio	Descripción																				
	<p>Control 1 “Los operadores de DataCenter, <i>trimestralmente</i> realizan la verificación (sic) y monitoreo de la capacidad de procesamiento, almacenamiento centralizado (SAN - NAS) y redes de datos, mediante herramientas de monitorización. En caso de verificar que los recursos están (sic) dentro los umbrales mínimos, (sic) informan al Subdirector Técnico (sic) de Recursos Tecnológicos (sic) para tomar las medidas correspondientes. Como evidencia se dejan los registros en el formato FO-TI-30”. (Subrayado fuera de texto).</p>	<p>datos tiene la STRT originando la materialización de riesgos de gestión o de seguridad de la información del proceso.</p> <p>Las situaciones identificadas son:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th style="text-align: center;">Trimestre</th> <th style="text-align: center;">Fechas en las que debió realizarse la toma de datos de capacidad</th> <th style="text-align: center;">Fecha de toma Datos de capacidad</th> <th style="text-align: center;">Retraso en la medición (En días hábiles)</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td>Entre el 3 y el 7 de enero de 2022 inclusive</td> <td style="text-align: center;">21/01/2022</td> <td style="text-align: center;">9</td> </tr> <tr> <td style="text-align: center;">2</td> <td>Entre el 1 y el 7 de abril de 2022 inclusive</td> <td style="text-align: center;">10/05/2022</td> <td style="text-align: center;">21</td> </tr> <tr> <td style="text-align: center;">3</td> <td>Entre el 1 y el 8 de julio de 2022 inclusive</td> <td style="text-align: center;">24/07/2022</td> <td style="text-align: center;">10</td> </tr> <tr> <td style="text-align: center;">4</td> <td>Entre el 3 y el 7 de octubre de 2022 inclusive</td> <td style="text-align: center;">27/10/2022</td> <td style="text-align: center;">13</td> </tr> </tbody> </table> <p>Es de anotar que la STRT presentó unas mediciones de capacidad en un piloto del formato FO-TI-30, que, según lo indicado corresponden a 12 semanas, lo que significaría que se tomaron desde mediados o finales de septiembre de 2022. Sin embargo, en el archivo suministrado no es posible identificar la fecha de toma de las mismas, ya que ésta se visualiza como un número.</p>	Trimestre	Fechas en las que debió realizarse la toma de datos de capacidad	Fecha de toma Datos de capacidad	Retraso en la medición (En días hábiles)	1	Entre el 3 y el 7 de enero de 2022 inclusive	21/01/2022	9	2	Entre el 1 y el 7 de abril de 2022 inclusive	10/05/2022	21	3	Entre el 1 y el 8 de julio de 2022 inclusive	24/07/2022	10	4	Entre el 3 y el 7 de octubre de 2022 inclusive	27/10/2022	13
Trimestre	Fechas en las que debió realizarse la toma de datos de capacidad	Fecha de toma Datos de capacidad	Retraso en la medición (En días hábiles)																			
1	Entre el 3 y el 7 de enero de 2022 inclusive	21/01/2022	9																			
2	Entre el 1 y el 7 de abril de 2022 inclusive	10/05/2022	21																			
3	Entre el 1 y el 8 de julio de 2022 inclusive	24/07/2022	10																			
4	Entre el 3 y el 7 de octubre de 2022 inclusive	27/10/2022	13																			
H2	<p>MG-TI-016 MANUAL BACKUPS Y RECUPERACIÓN DE LA INFORMACIÓN, v 6.</p> <p>5 POLÍTICAS DE RESPALDO Y CONSERVACIÓN DE LA INFORMACIÓN “[...] <i>Realizar pruebas periódicas aleatorias para garantizar que las copias de seguridad funcionan correctamente y la información contenida es recuperable.</i> [...] <i>Las copias de seguridad que se hacen de la información estructurada, de las aplicaciones y de los repositorios de código fuente deben permanecer en el sistema de almacenamiento del equipo DR6000 durante al menos seis (6) meses.</i> [...]”. (Subrayado fuera de texto).</p> <p>6 ROLES Y RESPONSABILIDADES RELATIVAS A LAS COPIAS DE SEGURIDAD</p> <p>6.2 OPERADOR DE COPIAS DE SEGURIDAD Y BASE DE DATOS</p>	<p>Hallazgo 2. Incumplimiento de algunas actividades relacionadas con la gestión de copias de seguridad</p> <p>Se evidenció incumplimiento de algunas actividades relacionadas con la gestión de copias de seguridad como la presentación a la subdirectora de la STRT, de forma bimestral, de informes del estado de los trabajos de generación y restauración de copias de seguridad; la elaboración del plan de pruebas y la realización de pruebas periódicas aleatorias; y el tiempo mínimo de retención en el equipo DR6000 de los <i>jobs</i> de copias de seguridad “S3-MAR-BODEGA_ORFEO_2013” y “D1-BK03CC01_DB_BKEXEC”, hechos que contravienen los incisos sexto y octavo del numeral 5, el segundo ítem del numeral 6.2, y el numeral 8.8 del manual MG-TI-016 y el numeral 1.1.6.2 del procedimiento PR-TI-12; situaciones que podrían afectar la disponibilidad de la información para la operación de la entidad, en los casos en que sea necesario restaurar de copias de seguridad y el disponer de información consolidada sobre el estado de la gestión de copias para la toma de decisiones.</p>																				

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Nº	Criterio	Descripción												
	<p><i>El rol designado para realizar la operación de copias de seguridad, desarrolla las siguientes actividades:</i> “[...] • Presentar al Subdirector, informes de estado de los trabajos de copias de seguridad y restauración realizados, <u>de forma bimestral</u>”. (Subrayado fuera de texto).</p> <p>8.8 PROCESO DE VERIFICACIÓN DE LAS COPIAS DE SEGURIDAD</p> <p>“Con el fin de verificar y controlar que las copias de seguridad se encuentren en buen estado, <u>el administrador del centro de cómputo elaborará un plan de pruebas</u>. [...]” (Subrayado fuera de texto).</p> <p>PR-TI-12 RESTAURACIÓN DE COPIAS DE SEGURIDAD, v 1</p> <p>1.1.6.2 ¿Es un proceso de verificación?</p> <p>“[...] Las pruebas de efectividad o calidad del procedimiento de generación de copias deben ser “evaluadas” mediante <u>procesos periódicos de restauración</u> que se realizan según corresponda el tipo de copia generada. [...]”. (Subrayado fuera de texto).</p>													
H3	<p>DU-TI-01 CATÁLOGO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN, v 5.</p> <p>6 CATÁLOGO DE SERVICIOS Acuerdos Niveles de Servicio, numerales 6.1.8 Servicio Atención de Eventos de Tecnología</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #0070C0; color: white;">ANS Requerimiento</th> <th style="background-color: #0070C0; color: white;">Operación Normal</th> </tr> </thead> <tbody> <tr> <td style="background-color: #D9E1F2;">Tiempo de Atención</td> <td style="background-color: #D9E1F2;">30 minutos</td> </tr> <tr> <td style="background-color: #D9E1F2;">Tiempo de Solución</td> <td style="background-color: #D9E1F2;">120 minutos</td> </tr> </tbody> </table> <p>6.3.8 Servicio Soporte Sobre Aplicaciones de Software 6.9.8 Servicio Acceso Seguro a la Red Institucional</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #0070C0; color: white;">ANS Requerimiento</th> <th style="background-color: #0070C0; color: white;">Operación Normal</th> </tr> </thead> <tbody> <tr> <td style="background-color: #D9E1F2;">Tiempo de Atención</td> <td style="background-color: #D9E1F2;">30 minutos</td> </tr> <tr> <td style="background-color: #D9E1F2;">Tiempo de Solución</td> <td style="background-color: #D9E1F2;">120 minutos</td> </tr> </tbody> </table>	ANS Requerimiento	Operación Normal	Tiempo de Atención	30 minutos	Tiempo de Solución	120 minutos	ANS Requerimiento	Operación Normal	Tiempo de Atención	30 minutos	Tiempo de Solución	120 minutos	<p>Hallazgo 3. Debilidades en los tiempos de atención y solución de casos en mesa de ayuda en agosto de 2022.</p> <p>Se evidenciaron debilidades en los tiempos de atención y solución de casos registrados en mesa de ayuda, a través de la herramienta Aranda, en agosto de 2022, hechos que contravienen los numerales 6.1.8, 6.2.8, 6.3.8, 6.4.8, 6.5.8, 6.6.8, 6.7.8, 6.8.8, 6.9.8, 6.10.8, 6.11.8, 6.12.8, 6.13.8, 6.14.8, y 6.15.8 del documento DU-TI-01, situaciones que puede afectar la calidad del servicio ofrecido a los usuarios y la toma de decisiones en relación con la atención a los usuarios que hacen uso de los servicios de Tecnologías de la Información.</p> <p>Las situaciones evidenciadas fueron las siguientes:</p> <ul style="list-style-type: none"> Se encontraron 3.888 casos en los cuales la atención fue extemporánea pues, desde el registro, fueron superados los 30 minutos, con rangos de atención que oscilan desde los 31 minutos hasta los 34.753 minutos. Estos casos, cuya atención fue
ANS Requerimiento	Operación Normal													
Tiempo de Atención	30 minutos													
Tiempo de Solución	120 minutos													
ANS Requerimiento	Operación Normal													
Tiempo de Atención	30 minutos													
Tiempo de Solución	120 minutos													

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Nº	Criterio	Descripción												
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: center;">ANS Requerimiento</th> <th style="text-align: center;">Operación Normal</th> </tr> <tr> <td style="text-align: center;">Tiempo de Atención</td> <td style="text-align: center;">30 minutos</td> </tr> <tr> <td style="text-align: center;">Tiempo de Solución</td> <td style="text-align: center;">240 minutos</td> </tr> </table> <p>6.2.8 Servicio Instalación de Aplicaciones de Software 6.4.8 Servicio Préstamo de Equipos para Reuniones 6.5.8 Servicio Préstamo Sala Iducate 6.6.8 Servicio Digitalización de Documentos e Impresión en Gran Formato 6.7.8 Servicio Administración de Usuarios de Tecnología 6.8.8 Servicio Recursos Compartidos 6.10.8 Servicio Asignación de Permiso de Navegación En Internet 6.11.8 Servicio Configuración de Dispositivos Móviles 6.12.8 Servicio Plataforma Tecnológica para Capacitación Virtual 6.13.8 Servicio Generación de Copias de Seguridad por Demanda 6.14.8 Servicio Restauración de Copia de Seguridad por Demanda 6.15.8 Servicio Acompañamiento en la Formulación y Desarrollo de Proyectos Institucionales en el Componente de TI</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: center;">ANS Requerimiento</th> <th style="text-align: center;">Operación Normal</th> </tr> <tr> <td style="text-align: center;">Tiempo de Atención</td> <td style="text-align: center;">30 minutos</td> </tr> <tr> <td style="text-align: center;">Tiempo de Solución</td> <td style="text-align: center;">240 minutos</td> </tr> </table>	ANS Requerimiento	Operación Normal	Tiempo de Atención	30 minutos	Tiempo de Solución	240 minutos	ANS Requerimiento	Operación Normal	Tiempo de Atención	30 minutos	Tiempo de Solución	240 minutos	<p>extemporánea, representan el 70,29 % sobre el total de casos.</p> <ul style="list-style-type: none"> En el campo “<i>TIEMPOSOLUCION</i>” se encontraron 2.932 casos cuyo tiempo de solución fue superior a 240 minutos, valor que se tomó por ser el más común a los diferentes servicios que presta la STRT en operación normal. Estos casos representan el 53,3 % del total de casos registrados en agosto de 2022 para atención en mesa de ayuda. <p>El detalle de los casos identificados, están registrado en el Anexo N.º 2 Debilidades en tiempos de atención (ANS), Casos agosto 2022.</p>
ANS Requerimiento	Operación Normal													
Tiempo de Atención	30 minutos													
Tiempo de Solución	240 minutos													
ANS Requerimiento	Operación Normal													
Tiempo de Atención	30 minutos													
Tiempo de Solución	240 minutos													
H4	<p>MG-TI-18 MANUAL OPERATIVO POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</p> <p>6.3.5.5.3 Retiro definitivo de los derechos de acceso a los servicios de TI.</p> <p><i>“Se les debe suspender el acceso a los servicios de TI a los servidores públicos o contratistas de prestación de servicios cuando pierden su vinculación con la entidad. [...]”.</i></p> <p>DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN</p> <p>6.10. Desvinculación de funcionarios y contratistas de apoyo a la gestión</p>	<p>Hallazgo 4. Usuarios de red activos de 2 exfuncionarios de la Entidad.</p> <p>Se evidenciaron 2 exfuncionarios del IDU que a 19/12/2022 continuaban con el usuario de red activo, contraviniendo lo establecido en el numeral 6.3.5.5.3 del manual MG-TI-18 y el numeral 6.10 del documento de políticas operacionales DU-TI-06, lo cual podría afectar la confidencialidad e integridad de la información del Instituto al existir la posibilidad de que, con el uso de estos usuarios de red, se realicen operaciones en los sistemas de información.</p> <p>Al realizar el cruce de información de los listados de usuarios de red activos e inactivos, suministrados por la STRT (archivos “<i>Usuarios Activos.xlsx</i>” y “<i>Usuarios Activos.xlsx</i>”), con el listado de funcionarios retirados en 2022, suministrado por la STRH (archivo “<i>Ingresos - Retiros</i>”</p>												

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO FO-EC-111	PROCESO EVALUACIÓN Y CONTROL	VERSIÓN 1.0	

Nº	Criterio	Descripción
	<p>“El facilitador del área debe solicitar la desactivación de las credenciales de acceso del usuario que se retira de la entidad tan pronto esto ocurra.</p> <p>Una vez se radique la solicitud de desactivación de las credenciales del usuario, la Subdirección Técnica de Recursos Tecnológicos procederá a desactivarlas. Bajo esta premisa, la persona que poseía dichas credenciales no podrá volver a hacer uso del ingreso a la red institucional, a los sistemas de información, a las aplicaciones, así como tampoco al servicio de correo electrónico. [...]”.</p>	<p>2022.xlsx”), se identificaron los siguientes exfuncionarios con usuario de red activo:</p> <ul style="list-style-type: none"> • 13XXX445 Uriel M. C.: renuncia desde el 14/07/2022. Se encontró solicitud de terminación de permisos de usuario en Gestión TIC y el respectivo caso Aranda. • 52XXX219 Marcia A. B. P.: terminación del nombramiento desde el 08/02/2022. Se encontró solicitud de terminación de permisos de usuario en Gestión TIC y el respectivo caso Aranda. <p>Cabe anotar que el último caso también contaba, a 19/12/2022 con el usuario Orfeo activo.</p>
H5	<p>PR-TI-06 GESTIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN, v 5</p> <p>1.1.19. Seguimiento, monitoreo y control</p> <p>“Con la información almacenada en la Base de Datos de Aranda se realizan análisis mensuales de la calidad del servicio prestado, <u>basados en los acuerdos de nivel de servicio (ANS)</u>. Se tienen en cuenta tanto cantidad de eventos y/o solicitudes, como satisfacción del servicio por parte del usuario final.</p> <p>Quando se detectan situaciones que pueden afectar o mejorar la prestación del servicio, se toman acciones para solucionar las situaciones evidenciadas.” (Subrayado fuera de texto).</p> <p>CP-TI-01 CARACTERIZACIÓN PROCESO TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN, v 6.</p> <p>Actividad crítica 9. Seguimiento a la Gestión 6. Informe de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio - ANS</p>	<p>Hallazgo 5. Falta de análisis de tendencias de cumplimiento en el producto “6. Informe de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS”</p> <p>Se evidenció que en el informe de ejecución de mesa de servicios de junio de 2022, si bien se presentan estadísticas de cantidad de casos atendidos frente a diferentes variables como especialistas o categorías, no se está presentando un análisis de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS, lo cual contraviene lo establecido en el numeral 1.1.19 del procedimiento PR-TI-06 y la salida 6 de la actividad 9 de caracterización del proceso CP-TI-01, hecho que no permite identificar situaciones que pueden afectar o mejorar la prestación del servicio desde el punto de vista del tiempo de atención y limita la toma de decisiones en este aspecto.</p>

4. RECOMENDACIONES/ OPORTUNIDADES DE MEJORA

1. Adaptar los lineamientos establecidos en la Guía G.ES.06 Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI a la casuística del IDU, evitando la transcripción literal de algunos contenidos de la misma en temas relevantes como el objetivo del PETI.
2. Definir, para el PETI, objetivos específicos más explícitos que permitan su adecuado seguimiento.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

3. Desarrollar al capítulo 6. ENTENDIMIENTO ESTRATÉGICO del PETI en concordancia con los contenidos del capítulo 7. ANÁLISIS DE LA SITUACIÓN ACTUAL.
4. Cuantificar de manera completa el PETI en el periodo para el que se formula, para el caso en comento, el cuatrienio 2021-2024, de manera que se determinen las necesidades de dicho periodo y se estime la totalidad de recursos necesarios para su cumplimiento.
5. Seguir el lineamiento de la Guía G.ES.06 y realizar las actualizaciones al PETI anualmente, sin exceder los doce meses, por cuanto periodos más amplios, como el que se presenta entre la expedición de las versiones 14 (enero de 2021) y 15 (diciembre de 2022), hacen que muchos de los componentes pierdan actualidad durante la vigencia de la versión correspondiente.
6. Revisar las observaciones registradas en este informe y los detalles expresados en las reuniones de auditoría para fortalecer el PETI y presentar una versión mejorada, en lo posible en la número 15, toda vez que, al no haber sido publicada, podría ser revisada nuevamente por el Comité Institucional Gestión y Desempeño para contar, en la vigencia 2023, con un documento actualizado y más alineado a los criterios propuestos en la Guía G.ES.06 del MinTIC.
7. Verificar la pertinencia de la desagregación contractual para futuros procesos contractuales como los descritos en el ítem 11 asociados a *“Adquisición de licencias nuevas y renovación, soporte, actualización y mantenimiento (SAM) de software especializado para procesos de ingeniería en infraestructura civil y de movilidad del IDU”*.
8. Verificar los aspectos técnicos que están generando fallas en el control *“sistema de autenticación basado en el directorio activo”* del riesgo C.TI.01.
9. Actualizar la descripción de los controles para la inclusión de la modalidad de acceso, a sistemas de información o recursos de TI, que no se registran en CHIE: Gestión TIC, por cuanto se está limitando el control a una única forma de registro previo de las autorizaciones.
10. Efectuar el ajuste que corresponda, ya sea en el Instructivo IN-TI-16 o en la matriz de riesgos de corrupción, para asegurar la consistencia en la operación del control relacionado con la revisión de los derechos de acceso a los recursos de TI con la documentación respectiva.
11. Revisar, y en lo posible, ajustar la información asociada a variables contenidas en la matriz de riesgos de corrupción y de gestión, de acuerdo con lo señalado en este informe, en especial, a la definición del riesgo, causas, diseño de controles, definición de responsables, entre otros.
12. Determinar claramente los cargos y roles de quienes ejecutan los controles asociados a los riesgos del proceso, ajustarlos frente a la metodología que se esté aplicando, de manera que se constituya en un elemento de control efectivo y queden las evidencias correspondientes.
13. Sistematizar el registro de las solicitudes de copias de seguridad para identificar la completitud de su aplicación.
14. Efectuar las correcciones para complementar la información de descripción del control 7 del riesgo G.TI.03, así como realizar las acciones respectivas ante la OAP para que se vean reflejadas en la matriz de riesgos publicada en la Intranet.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

15. Dejar registros de la ejecución periódica de los controles asociados a los riesgos del proceso.
16. Socializar con la Oficina Asesora de Planeación – OAP los resultados registrados en este informe, frente al componente de riesgos.
17. Asegurar que, una vez se apruebe el piloto de la nueva automatización del formato de control de la capacidad FO-TI-30, se efectúen las gestiones que correspondan en el sistema de información documentada SUE para el ajuste y actualización de versión.
18. Asegurar que los datos registrados en el formato de control de la capacidad FO-TI-30 sean legibles y obedezcan a estándares o patrones reconocibles para quienes hagan uso del mismo, resguardando la integridad de su contenido.
19. Documentar los criterios para determinar a qué recursos es importante o fundamental hacerle la medición de capacidad.
20. Asegurar que la información necesaria para la gestión de la capacidad, ya sea registrada de forma manual o automatizada, y otra que sea relevante para el efecto, esté almacenada y organizada de tal forma que sea de fácil acceso para aquellos que la requieran y en el momento que se necesite, cumpliendo, naturalmente, con los criterios de confidencialidad e integridad.
21. Establecer un periodo de tiempo específico para asegurar que cada año, en las mismas fechas, se realice la verificación del nivel de obsolescencia de los elementos de TI y que ésta contribuya a la toma de decisiones relacionadas con la gestión de la capacidad.
22. Completar la información del formato de hoja de vida de servidores lo más pronto posible e incluir información de trazabilidad del diligenciamiento de cada ficha, agregando, para aquellos activos en los que no aplique cierta información, un dato que permita inferirlo.
23. Revisar la documentación relacionada con el tema de copias de seguridad para efectuar el ajuste de inclusión de la actividad de copia de las bases de datos a un servidor específico para hacerle, a éste, la copia a cinta y asegurar que las actividades de *backup* se realicen según como están documentadas.
24. Documentar las excepciones aplicables en el uso de los formatos FO-TI-218 “*Solicitud Realización de Backup*” y FO-TI-185 “*Solicitud de Restauracion de Backup*”, por ejemplo, en el caso de las solicitudes efectuadas por personal del mismo proceso para pruebas de software.
25. Revisar los tiempos de solución de los servicios “*Servicio soporte sobre aplicaciones de software*” y “*Servicio acceso seguro a la red institucional*” y “*Servicio digitalización de documentos e impresión en gran formato*” y efectuar los ajustes pertinentes para evitar ambigüedades.
26. Efectuar una revisión de la parametrización del sistema Aranda para que haya coincidencia entre los servicios y ANS del catálogo de servicios DU-TI-01 con los tiempos estimados y jerarquías / categorías del sistema.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

27. Reforzar la capacitación sobre el sistema CHIE: Gestión TIC, de manera que se propenda porque el tipo de solicitud de cada caso registrado corresponda con la definición establecida.
28. Revisar la configuración para el envío de las encuestas de evaluación del servicio prestado por la mesa de ayuda frente a la atención de algún caso y evaluar la posibilidad de implementar una solución de encuestas que se pueda responder desde cualquier ubicación.
29. Buscar estrategias que logren el incremento en el número de encuestas de evaluación del servicio respondidas, o maneras diferentes para que se pueda realizar tal evaluación.
30. Realizar las mediciones del indicador interno de la STRT "*Percepción de la prestación del servicio de soporte de TI*" pertinentes para medir el nivel de satisfacción de los usuarios en la prestación del servicio.
31. Actualizar los valores correspondientes al segundo y tercer trimestre de 2022, del indicador "*Percepción de la prestación del servicio de soporte de TI*" en la información Excel que se reporta a la Oficina Asesora de Planeación.
32. Realizar los ajustes de los indicadores PAE pertinentes para que las metas sean más coherentes con los resultados obtenidos, dado que éstas pueden estar subestimadas.
33. Tener en cuenta las observaciones de la OAP frente a las acciones de PAE, para complementar la información de reporte y facilitar el análisis de los resultados.
34. Efectuar las aprobaciones faltantes respecto de los activos de información del usuario Wilser H. P. S.
35. Realizar seguimiento a los 2 casos señalados en el informe, atinente a los usuarios identificados con cédula de ciudadanía 79XXX807 y 19XXX876, a fin de tomar las acciones pertinentes para finalizar los permisos de usuario.

5. CONCLUSIONES

En términos generales, se identificó la existencia y aplicación de controles en el proceso de Gestión de Tecnologías de Información y Comunicación, para las actividades descritas en el alcance de la auditoría. Se destaca la gestión del proceso en la búsqueda de innovación en algunas de las actividades que realizan. No obstante, de acuerdo con las actividades verificadas y los criterios establecidos para la auditoría, se evidenciaron requisitos con incumplimiento asociados con:

- Extemporaneidad en la revisión y actualización de valores de la capacidad de algunos elementos de TI (servidores de bases de datos, servidores de aplicaciones, servidores de almacenamiento, entre otros).
- Incumplimiento de algunas actividades relacionadas con la gestión de copias de seguridad.
- Debilidades en los tiempos de atención y solución de casos en mesa de ayuda en agosto de 2022.
- Usuarios de red activos de 2 exfuncionarios de la Entidad.

FORMATO			
INFORME DE AUDITORIA			
CÓDIGO	PROCESO	VERSIÓN	
FO-EC-111	EVALUACIÓN Y CONTROL	1.0	

- Falta de análisis de tendencias de cumplimiento en el producto “6. Informe de tendencias de cumplimiento de los Acuerdos de Nivel de Servicio – ANS”.

A continuación, se relaciona el número de hallazgos y recomendaciones identificadas:

Total N.º Conformidades	Total Recomendaciones/ Oportunidades de mejora
5	35

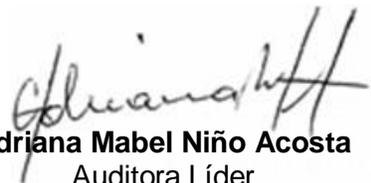
6. ANEXOS

- N.º 1 Análisis de riesgos de gestión y corrupción – Gestión de TIC.
 N.º 2 Debilidades en tiempos de atención (ANS), Casos agosto 2022.

7. EQUIPO AUDITOR



Ismael Martínez Guerrero
Jefe Oficina de Control Interno



Adriana Mabel Niño Acosta
Auditora Líder

No registra firma en atención a que se encuentra disfrutando del descaso compensado

Camilo Oswaldo Barajas Sierra
Auditor

No registra firma en atención a que se encuentra disfrutando del descaso compensado

Fernando Garavito Guerra
Auditor