ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Instituto de Desarrollo Urbano

MEMORANDO

OCI
20191350425003
Información Pública
Al responder cite este número

FECHA: Bogotá D.C., diciembre 13 de 2019

PARA: **Yaneth Rocío Mantilla Barón**
Directora General

DE: Jefe Oficina de Control Interno

REFERENCIA: Informe Final de Auditoría 2019 al Proceso de Gestión de las Tecnologías de Información y Comunicación

Respetada doctora Yaneth Rocío:

Reciba un cordial saludo. En cumplimiento del Decreto 648 de 2017 y el Decreto Distrital 215 de 2017, en relación con el destinatario principal de los informes de auditoría, seguimientos y evaluaciones, se remite el informe de la auditoría realizada al Proceso de Gestión de las Tecnologías de Información y Comunicación, en desarrollo del Plan Anual de Auditoría 2019, luego de haberse surtido la fase de comunicación y retroalimentación del Informe Preliminar, el cual fue comunicado mediante correo electrónico del 4 de diciembre de 2019, y quedó en firme dado que no fueron presentadas observaciones al mismo.

Este documento se informa a la Subdirección General de Gestión Corporativa – SGGC, como dependencia líder del proceso auditado; a la Dirección Técnica Administrativa y Financiera – DTAF y a la Subdirección Técnica de Recursos Tecnológicos – STRT en su condición de líderes operativos, y a la Oficina Asesora de Planeación – OAP, según solicitud efectuada mediante memorando 20171150244353.

Adicionalmente, se copia a la Dirección Técnica de Gestión Contractual – DTGC en consideración a que el Hallazgo N.° 4 “Ausencia y/o extemporaneidad en la publicación en SECOP de información contractual” es de responsabilidad de dicha dependencia.

Es necesario que las dependencias responsables formulen, a partir de los hallazgos evidenciados y en conjunto con las áreas pertinentes, un único plan de mejoramiento que contenga las correcciones, las acciones correctivas y/o de mejora 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”, versión 7.0, ubicado en la intranet, en la siguiente ruta:

Calle 22 No. 6 - 27
Calle 20 No. 9 – 20 o
Carrera 7ª No. 17-01 Piso 3
Código Postal 110311- 110321
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195

ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Instituto de Desarrollo Urbano

MEMORANDO

OCI
20191350425003
Información Pública
Al responder cite este número

http://intranet/manualProcesos/Mejoramiento_Continuo/03_Procedimientos/PRMC01_FORMULACI%C3%93N_MONITOREO_Y_SEGUIMIENTO_A_PLANES_DE_MEJORAMIENTO_V_7.pdf

Para elaborar el plan de mejoramiento se debe emplear el formato FO-MC-01 PLAN DE MEJORAMIENTO, versión 6.0, y es necesario diligenciar, previamente, uno de los instrumentos de análisis de causas que se encuentran dentro del mismo, tales como: lluvia de ideas, diagrama causa efecto y los cinco por qué. El mencionado formato se encuentra en la siguiente ruta:

http://intranet/manualProcesos/Mejoramiento_Continuo/05_Formatos/FOMC01_PLAN_DE_MEJORAMIENTO_INTERNO_V_6.0%20.xlsm.

De acuerdo con lo establecido en la política operacional del procedimiento de planes de mejoramiento antes 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.

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

Cualquier información adicional, con gusto será atendida.

Cordialmente,

Ismael Martínez Guerrero
Jefe Oficina de Control Interno
Firma mecánica generada en 13-12-2019 02:23 PM

Anexos: Informe Final de Auditoría Gestión de las TIC y sus anexos

cc Salvador Mendoza Suarez - Dirección Técnica Administrativa y Financiera
cc Leydy Yohana Pineda Afanador - Subdirección Técnica de Recursos Tecnológicos
cc Ligia Stella Rodríguez Hernández - Subdirección General de Gestión Corporativa
cc Isauro Cabrera Vega - Oficina Asesora de Planeación
cc Ivan Abelardo Sarmiento Galvis - Dirección Técnica de Gestión Contractual

Elaboró: Adriana Mabel Niño Acosta - Oficina de Control Interno

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 55548 de julio 29 de 2015

Calle 22 No. 6 - 27
Calle 20 No. 9 – 20 o
Carrera 7ª No. 17-01 Piso 3
Código Postal 110311- 110321
Tel: 3386660 - 3445000
www.idu.gov.co
Info: Línea: 195

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

1. INFORMACIÓN GENERAL

Tipo de Informe	**Preliminar** ☐	**Final** X	**Fecha de elaboración del informe:**	13/12/2019
Proceso/Objeto Auditado	Proceso de Gestión de las Tecnologías de Información y Comunicación			
Líder del proceso/ Cargo y dependencia	Subdirector General de Gestión Corporativa - SGGC			
Líder operativo del Proceso/ cargo y dependencia	Director Técnico Administrativo y Financiero Subdirector Técnico de Recursos Tecnológicos			
Tipo de Auditoría	Auditoría de gestión			
Objetivo	Evaluar la gestión del proceso Gestión de las Tecnologías de Información y Comunicación, a través de la verificación del cumplimiento de la normatividad legal y reglamentaria y directrices institucionales aplicables a las actividades del proceso, a fin de identificar aspectos que contribuyan a su mejoramiento continuo.			
Alcance	La presente auditoría tuvo como alcance las verificaciones de soportes, registros y documentación asociada con las actividades críticas establecidas en la caracterización del Proceso Gestión de las Tecnologías de Información y Comunicación, haciendo énfasis en las siguientes: • Actividad N.° 2 “Administración de Infraestructura de T.I.”. • Actividad N.° 8 “Continuidad de servicios de TI (Recuperación ante desastres)”. • Actividad N.° 9. “Seguimiento a la Gestión”. • Actividad N.° 10 “Optimización del proceso”. La evaluación se circunscribió, principalmente, a la verificación de la gestión de copias de respaldo (generación y restauración), de la operación de la estrategia de recuperación ante desastres de los servicios de TI y seguridad de la información y seguimiento a riesgos y Plan de mejoramiento del proceso. Adicionalmente, se abordó la revisión de contratos relacionados con los temas citados. El periodo de verificación comprendió desde el 01/01/2019 hasta el 31/10/2019; no obstante, en materia contractual, se revisaron contratos de la vigencia 2018. Las actividades de auditoría se basaron en la verificación de información suministrada por el proceso (entregada en medio físico, digital y/o entrevistas) y la información consultada en sistemas de información aplicables al proceso, en la intranet o la página web del IDU, entre otras fuentes.			

Criterios de Auditoría	• Normograma del proceso de Gestión de las Tecnologías de Información y Comunicación. • Información documentada del proceso (procedimientos, guías, instructivos, manuales, formatos, entre otros), publicada en la intranet institucional, o la aplicable en el periodo de evaluación. • Demás documentación del Manual de Procesos de IDU y normatividad legal y reglamentaria, que aplique al proceso y actividades evaluadas.
Fecha reunión de apertura	15/11/2019
Fecha reunión de cierre	05/12/2019 (por realizar)
Equipo auditor/ Dependencia/ Rol	Adriana Mabel Niño Acosta, Profesional Especializado 222-05, Auditor Líder Erika María Stipanovic Venegas, Profesional Especializado 222-04, Auditor Acompañante

2. METODOLOGÍA

Esta auditoría se adelantó de conformidad con el plan presentado en la reunión de apertura, llevada a cabo el 15/11/2019 y formalizado mediante memorando 20191350393553 del 14/11/2019.

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.
- Entrevistas a los funcionarios y colaboradores 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.
- Solicitudes de información a través de correos electrónicos y soportes de actas de visita.
- Consulta de información en sistemas de información como el Sistema de Gestión Documental ORFEO, el Sistema de Información y Acompañamiento Contractual – SIAC, CHÍE: Plan Mejoramiento Institucional, SECOP I o II, entre otros.
- Revisiones *in situ* relacionadas con las actividades relacionadas y los contratos seleccionados, para verificar su conformidad, de acuerdo con la normatividad legal y los procedimientos internos vigentes.

A continuación, se relacionan los aspectos evaluados por cada una de las actividades y temáticas mencionadas en el alcance del Plan de auditoría, atendiendo descrito en la caracterización del proceso de Gestión de las Tecnologías de Información y Comunicación:

- Actividad N.° 2 “Administración de Infraestructura de T.I.”: verificación de la gestión de copias de respaldo (generación y restauración).
- Actividad N.° 8 “Continuidad de servicios de TI (Recuperación ante desastres)”: verificación de la operación de la estrategia de recuperación ante desastres de los servicios de TI y seguridad de la información.
- Actividad N.° 9. “Seguimiento a la Gestión”: seguimiento a riesgos del proceso.
- Actividad N.° 10 “Optimización del proceso”: plan de mejoramiento del proceso.

- Se abordó, además, la revisión de contratos relacionados con los temas citados, como sigue:

Para la selección de la muestra de contratos bajo la coordinación de la Subdirección Técnica de Recursos Tecnológicos - STRT, se tomaron aleatoriamente, de las bases de datos de las vigencias 2018 y 2019, contratos cuyo objeto coincidiera con el tema auditado y cuya ejecución se desarrolló total o parcialmente en el 2019, cuatro (4) contratos, que corresponden a:

Tabla N° 1. Selección de la muestra contractual

Ítem	N°. de contrato	Objeto
1	IDU-1520-2018	Adquisición de software especializado que permita la gestión de permisos, seguimiento a recursos, carpetas y archivos de datos no estructurados
2	IDU-1522-2018	Adquirir una solución de mitigación de ataques de denegación de servicio distribuido anti -DDOS
3	IDU-PSP-1298-2019	Prestar servicios profesionales para apoyar los asuntos relacionados con los servicios de tic, para identificar problemas que surjan en los controles de seguridad establecidos para salvaguardar la confidencialidad, integridad y disponibilidad de la información del Instituto.
4	IDU-1580-2019	Contratar el servicio de pruebas de hacking ético a la infraestructura tecnológica e ingeniería social al personal del IDU.

Fuente: Consolidación equipo auditor.

La revisión legal de los contratos seleccionados abarcó la verificación inicial de registros en el Sistema ORFEO, en el SIAC y las plataformas SECOP I o II, según cada caso en particular en aspectos generales como: consistencia del contrato frente a los documentos de adjudicación, incorporación de cláusulas de confidencialidad, suscripción del contrato, cumplimiento de requisitos de perfeccionamiento y ejecución, acta de inicio, ejecución contractual, obligaciones específicas a cargo del contratista, modificaciones contractuales (si a ello hubiese lugar), publicaciones, requisitos de pago, entre otros. De la revisión descrita, surgieron interrogantes para el equipo auditor, que fue necesario absolverlos a través de solicitudes específicas de información mediante correos electrónicos y entrevistas en el área auditada, que son descritas en el desarrollo de este informe; se precisa que se excluye en este acápite la revisión del componente técnico de los proyectos.

3. RESULTADOS DE LA AUDITORÍA

A continuación, se presentan los resultados para cada una de las actividades sujetas de verificación:

Actividad N.° 2 “Administración de Infraestructura de T.I.”

La revisión de esta actividad crítica se circunscribió a la verificación de la gestión de copias de respaldo (generación y restauración).

El proceso cuenta con los siguientes documentos relacionados con la gestión de copias de respaldo:

Tabla N° 2. Documentación asociada a la gestión de copias de respaldo

Nombre	Tipo de Documento	Código	Versión	Fecha
Manual de Generación y Restauración de Copias de Seguridad (adoptado mediante Resolución 494 de 2017)[1]	Manual	MG-TI-16	3.0	08/02/2017
Generación de Copias de Seguridad	Procedimiento	PR-TI-11	1.0	24/12/2014

[1] Radicado Orfeo 20171150004946.

Nombre	Tipo de Documento	Código	Versión	Fecha
Restauración de Copias de Seguridad	Procedimiento	PR-TI-12	1.0	24/12/2014
Solicitud de Restauración de *Backup*	Formato	FO-TI-185	3.0	08/07/2016
Solicitud Realización de *Backup*	Formato	FO-TI-218	3.0	08/07/2016

Fuente: Intranet, Mapa de Procesos. **Elaboración:** Equipo Auditor.

Como criterio principal para realizar la respectiva verificación se tomó el Manual de Generación y Restauración de Copias de Seguridad, código MG-TI-16, V 3.0 del 08/02/2017, aunque también se revisaron algunos aspectos de los procedimientos mencionados en la tabla anterior.

Mediante entrevistas con funcionarios y colaboradores de la Subdirección Técnica de Recursos Tecnológicos (STRT) y revisión en la herramienta de copias de seguridad que se utiliza en el Instituto, se verificó que dicha dependencia tiene establecida la toma de copias de seguridad de las aplicaciones, información estructurada (bases de datos) y otros repositorios de información (por ejemplo, carpetas compartidas, código fuente).

Es de aclarar que en las verificaciones efectuadas se pudo evidenciar que dicho manual se encuentra en gestión de actualización al interior de la STRT, específicamente en revisión por parte de personal del grupo de Infraestructura[2]; no obstante, al 02/12/2019, no se encontraba cargado en el sistema SUÉ: Información Documentada[3]. De acuerdo con lo manifestado por el proceso, se espera que el 11/12/2019 el documento inicie su trámite formal de actualización en el mencionado sistema.

Dado que el manual, en su versión 3.0, fue adoptado por la Resolución 494 de 2017 de la Dirección General, se recomienda confirmar cuál es el procedimiento adecuado para adoptar la versión que resulte de la actualización con el fin de asegurar que no vayan a permanecer dos manuales vigentes. Esto es, confirmar si es necesario efectuar la modificación o derogación de la mencionada resolución, tomando, también, en consideración lo indicado en el numeral "*6.1 MANUAL*" de la Guía "Documentación MIPG-SIG", código GU-AC-01 respecto a los manuales de gestión y manuales operativos.

Así mismo, es de mencionar que en la auditoría al Sistema Integrado de Gestión (SIG) del Instituto realizada en 2018, se revisaron aspectos del mismo manual, que llevaron a acciones de mejoramiento relacionadas con la elaboración de cronograma para la toma de copias de seguridad; la presentación de informes sobre la generación de copias de seguridad; y el control, por parte de la STRT, de que el área encargada de la supervisión[4] del contrato de almacenamiento y custodia de los medios magnéticos verifique que el contratista cumpla con las obligaciones relacionadas. Estas acciones de mejoramiento se describen más adelante, en el aparte referido a la Actividad N.° 10 "Optimización del proceso".

[2] La STRT, funcionalmente, se encuentra estructurada en diferentes grupos de trabajo, a saber: Apoyo a la gestión TIC, Arquitectura, Proyectos SI, Mesa de Servicio e Infraestructura. Fuente: Instituto de Desarrollo Urbano – IDU. "Plan Estratégico de Tecnologías de Información y Comunicación – PETI, versión 11.0", enero de 2019, pág. 35.

[3] El módulo "Información Documentada" del sistema de información SUÉ es un aplicativo web, desarrollado en la plataforma Odoo (antes OpenERP), mediante el cual se lleva a cabo la gestión o trámite de la documentación del Sistema Integrado de Gestión del IDU (por ejemplo, solicitud de creación, actualización y/o derogación de documentos, control de versionamiento, etc.).

[4] El área encargada es la Subdirección Técnica de Recursos Físicos.

Como parte de la revisión de los documentos mencionados en la Tabla N° 2 se encontró desactualización en los numerales "*1.1.3 Marco Normativo*" de los procedimientos PR-TI-11 "Generación de Copias de Seguridad" y PR-TI-12 "Restauración de Copias de Seguridad" y del numeral "*4. Marco Normativo*" del Manual de Generación y Restauración de Copias de Seguridad, código MG-TI-16, V 3.0, como sigue:

- En los tres documentos citan 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 fue derogada por la Resolución IDU 852 de 2019 (marzo 8), a su vez derogada por la Resolución IDU 1641 de 2019 (abril 26).

- También, citan la Resolución 305 de 20 de octubre de 2008 "*Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre*", la cual fue modificada por la Resolución 004 de 2017 (noviembre 28) de la Comisión Distrital de Sistemas (CDS). Sin embargo, esta resolución no está incluida.

- El Manual cita la "*Resolución interna 64994 DE 2015 "Por medio de la cual se actualiza el modelo de operación por procesos y el Sistema Integrado de Gestión del IDU"*" (sic), que fue derogada mediante Resolución 3807 de 2017 (julio 25), a su vez derogada por la Resolución 1303 de 2019 (abril 1), también derogada por la Resolución 1909 de 2019 (mayo 14).

Se recomienda, entonces, tener en cuenta en la actualización del Manual y los procedimientos relacionados con generación y restauración de copias de seguridad, la revisión del Marco Normativo, de manera que se agregue la normatividad faltante y se elimine y/o reemplacen las normas derogadas o que no apliquen por las vigentes.

Se verificó que, para la toma de copias de seguridad, la STRT tiene destinado el servidor DELL POWER EDGE- R730 identificado con el nombre "BK03CC01", el cual tiene Windows 2012 Server R2 como sistema operativo. El software empleado es Symantec Backup Exec TM 15, conforme lo indicado en los numerales "*8.1.1 Dispositivos para la Toma de Copias*" y "*8.2 Software*" del Manual de Generación y Restauración de Copias de Seguridad, código MG-TI-16, versión 3.0.

Igualmente, en relación con las Áreas de Almacenamiento (numeral 8.1.2), el operador de centro de cómputo entrevistado indicó que la infraestructura actualmente utilizada es la indicada en el manual, a saber:

"***SISTEMA DE ALMACENAMIENTO A DISCO***
Nombre máquina: DELL - DR6000.
Tecnología: Disco Nearline SAS de 3,5 pulgadas.
Capacidad: 20 TB efectivas.
Tipo de Discos: Discos 7.2 K — 3 TB.

SISTEMA DE ALMACENAMIENTO A CINTA
Librerías: SL 150 ORACLE.
Tecnología: LTO 6.
Capacidad máxima: 2.50/6.25TB por cinta.

Cantidad de drives: 3 drives.
Capacidad de cintas: 90 cintas."

El operador de centro de cómputo entrevistado indicó que no se utiliza ninguna otra herramienta.

En las "*POLÍTICAS DE RESPALDO Y CONSERVACIÓN DE LA INFORMACIÓN*" (numeral 6.) del citado manual está mencionado que (cuarto inciso): "*Semestralmente se establecerá una planeación para la toma de copias de seguridad, la cual deberá ser realizada por el administrador del centro de cómputo y/o el líder del grupo funcional de infraestructura*".

De igual manera, en el numeral "*7.1 Administrador del centro de cómputo*" del manual está indicado:

"*El rol designado para realizar la administración del centro de cómputo desarrolla las siguientes actividades*: […]

• *Realizar cronograma de actividades para la toma de las copias de seguridad y mantenerlo actualizado periódicamente.*

• […]".

Sin embargo, se identificó que la manera en la que se toman las copias de seguridad está configurada en la herramienta utilizada (Symantec Backup Exec 15) y se ajusta en casos derivados de situaciones tales como cambios en los sistemas de información o en la infraestructura que los soporta (que puede incluir eliminación de sistemas o de equipos), implementación de nuevos sistemas de información, o solicitudes específicas según necesidades identificadas en la STRT, entre otras, como lo indican las viñetas del inciso sexto de las mismas políticas.

Es decir, semestralmente, el administrador del centro de cómputo y/o el líder del grupo funcional de infraestructura, no establecen ni realizan una planeación para la toma de copias de seguridad, ni realizan cronograma de actividades para la toma de las copias de seguridad o lo actualizan periódicamente; de hecho, como se mencionó, la toma de copias de seguridad se ejecuta de acuerdo con lo parametrizado en la herramienta, sin obedecer a una planeación periódica y los ajustes de los parámetros se hace en casos puntuales.

Esto implica un incumplimiento de esta política, puesto que la planeación no se establece semestralmente y la toma de copias se realiza según la configuración en la herramienta. No obstante, dado que la STRT ya inició la revisión y actualización del manual, no se genera un hallazgo, sino que se recomienda considerar el ajuste de la política de planeación para la toma de copias de seguridad de acuerdo con la forma en la que efectivamente se realiza esta labor.

Por otra parte, si bien se verificó que se hacen copias de la información estructurada (bases de datos), de las aplicaciones y de los repositorios de información no estructurada (recursos compartidos o archivos) y de código fuente, se evidenció que el Manual sólo hace alusión a políticas para las copias de seguridad, en relación con la periodicidad de copiado y de retención en cinta, de las bases de datos de Oracle (ver inciso 9, pág. 11, del manual MG-TI-16).

Además, el Manual señala, en el séptimo inciso del numeral 6, que "[…]. *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*. […]". No obstante, se evidenció que este parámetro no está estándar para todos los recursos.

Por ejemplo, según la configuración en la herramienta de *backup*, se observó que el trabajo denominado "SQL_KACTUS_DIA_COMPLETA", programado para efectuarse todos los días a la 1:00 pm, se conserva en el DR6000 durante 25 semanas (aproximadamente 6 meses), mientras que el trabajo "ORACLE_EXPORTS_COMPLETA", programado para el último sábado del mes a las 8:15 am, se conserva durante 16 semanas (aproximadamente 4 meses).

Lo descrito significa que no está claro cuáles son las políticas aplicables para la toma y permanencia de copias de respaldo para las bases de datos que se encuentran en sistemas de gestión de bases de datos diferentes a Oracle (como SQL Server o PostgreSQL), tampoco para archivos o recursos compartidos, servidores web, servidores virtualizados, aplicaciones, o repositorios de código fuente.

De acuerdo con lo señalado por el operador de centro de cómputo entrevistado, el tipo (total o incremental) y la periodicidad de toma de copias de seguridad y la retención en cinta depende de la criticidad de los diferentes elementos o recursos a los cuales se les realiza la copia. No obstante, no están documentados los criterios o parámetros para determinar esa criticidad, de manera que se defina, con base en ella, cuál sería la periodicidad, tipo de *backup* o tiempo de retención adecuados para cada recurso. Por ejemplo, las bases de datos se consideran recursos críticos, pero es posible que no todas tengan la misma criticidad, dependiendo de su tamaño o del volumen de transacciones que se realicen sobre las mismas.

Por lo anterior, se recomienda establecer y documentar los criterios o parámetros para determinar la criticidad de los recursos o elementos a los cuáles se les toma copia de seguridad y, con base en ellos, identificar e incluir en las políticas de *backup* las relativas a la periodicidad y tipo de copiado, de tiempo de retención en cinta y/o de permanencia en el sistema de almacenamiento, aplicables a cada recurso o tipo de recurso.

Con respecto a los Roles y Responsabilidades Relativas a las Copias de Seguridad (numeral 7 del Manual MG-TI-16), se evidenció que si bien en el manual se diferencian las tareas que ejecuta el rol del Administrador del Centro de Cómputo (numeral 7.1) y con las del Operador de Copias de Seguridad (numeral 7.2), en la práctica las actividades específicas las están ejecutando indistintamente diferentes personas que laboran en la STRT. Esto se evidencia en lo siguiente:

- En la actualidad hay dos contratistas en la STRT que, según las indagaciones efectuadas, desarrollan el rol de administrador de centro de cómputo. Al indagar por quién desarrolla el rol de operador de copias de seguridad, la respuesta fue que los mismos dos contratistas desarrollan, también, este rol. Verificando el manual de funciones de la STRT, el rol de administrador de centro de cómputo lo efectuaría un profesional universitario 2019-02 (que corresponde al líder del grupo funcional de infraestructura de la Subdirección) y el de operador de copias de seguridad lo efectuaría un profesional universitario 2019-01.

- Las tareas de "*Mantener control sobre el almacenamiento de las copias de seguridad*" y "*Vigilar y controlar que el área encargada de supervisar el contrato de almacenamiento y custodia de los medios magnéticos en sitio externo, cumpla con las obligaciones pactadas con el IDU*" asignadas en el manual al rol de Administrador del Centro de Cómputo las está realizando una profesional universitaria, grado 219-01, que, de acuerdo con el manual de funciones de la STRT, no tiene asignado este rol.

Dado que las actividades asignadas, exceptuando se realizan, según lo mencionado previamente, la relativa a la realización del cronograma de actividades para la toma de las copias de seguridad, pero no se efectúan según los roles establecidos en el Manual, se sugiere revisar dichas actividades, conciliar con el manual de funciones de los profesionales de planta o las obligaciones de los contratistas y diferenciar, en la práctica, quién ejecuta cada rol.

Ahora bien, de acuerdo con lo establecido en el numeral "*9.4 Ubicación Física de las Copias de Seguridad*", se evidenció que en las instalaciones de la Subdirección Técnica de Recursos Tecnológicos, en el centro de cómputo tienen un espacio o gabinete, denominado "Cintoteca", donde permanecen las cintas llenas por un periodo, aproximado, de 6 meses. Así mismo, se verificó que el Instituto tiene vigente el contrato IDU-1376-2019 con la empresa TANDEM S.A.S., cuyo objeto es "*Prestar el servicio de almacenamiento y custodia de archivos y medios magnéticos del IDU en el marco del fortalecimiento de la gestión documenta*l". De acuerdo con lo registrado en el Sistema de Información de Acompañamiento Contractual – SIAC, el contrato inició el 13/06/2019 y finaliza el 12/06/2020 y la supervisión está a cargo de la Subdirectora Técnica de Recursos Físicos[5].

En cuanto al etiquetado de las cintas (numerales "*9.5 Metodología para el Etiquetado de las Cintas*" del Manual de Generación y Restauración de Copias de Seguridad, MG-TI-16, y "*1.1.6.15 Etiquetado del medio de almacenamiento*" del Procedimiento Generación de Copias de Seguridad, PR-TI-11), se evidenció que se utiliza el estándar definido por la STRT, el cual corresponde a la identificación de los volúmenes de almacenamiento mediante etiquetas de código de barras, como se observa en la siguiente imagen:

Imagen N° 1. Ejemplo etiquetado de cintas

Fuente: STRT, cinta 000772, copia de "ARCHIVOS_SS04CC01".

Para identificar el contenido de la cinta, la herramienta Symantec Backup Exec permite generar un reporte llamado "*Resumen de soportes*", en el cual se pueden observar datos como a qué recurso o elemento se le generó la copia de seguridad, las fechas, el tamaño, entre otros.

Imagen N° 2. Resumen de soportes, cinta 000772

Symantec Backup Exec™

Resumen de soportes

ARCHIVOS_SS04CC01

Etiqueta de soportes	Tipo de soportes	Asignado	Modificado	Crítico para el negocio	Totales					Actual
					Horas	Montajes	Errores recuperables	Errores irrecuperables	Escritura	Tamaño
000772	LTO	09/06/2019	03/11/2019	No	72,64	64	6	0	2.326,988 GB	2.326,964 GB

Fuente: STRT. Fragmento de un reporte de "Resumen de soportes".

[5] Dado que la supervisión no está a cargo de la STRT, este contrato no fue seleccionado en la muestra de contratos.

Ahora bien, en el numeral 9.5 del Manual MG-TI-16 está especificado que se lleva un "[…] *archivo de apoyo en donde se lleva el control de las cintas que contienen las copias de seguridad deben registrarse los siguientes datos:*

- *Objeto al que se le toma la copia de seguridad.*
- *Nombre de la base de datos a la que se le toma la copia de seguridad.*
- *Número de orden del dispositivo físico que está en proceso.*
- *Nombre del sistema de archivos al que se le toma la copia de seguridad.*
- *Secuencia del dispositivo físico dentro del proceso.*
- *Fecha proceso.*
- *Utilitario empleado para tomar la copia de seguridad.*
- *Observaciones de la copia de seguridad*".

No obstante, en el *Resumen de soportes* no se identifican con claridad la totalidad de los datos mencionados. No se evidenció un archivo específico de apoyo para el control de las cintas que incluya los aspectos mencionados en el numeral 9.5. Las planillas de transferencia de cintas al archivo central (formato "Inventario único documental", código FO-DO-17), en las cuales se relaciona el título (u objeto copiado), las fechas inicial y final y, en el campo de observaciones, el número de la cinta (código de barras), no corresponde a dicho archivo de control. Por lo cual, reiterando que el manual se encuentra en actualización, se recomienda verificar específicamente en qué archivo se debería llevar el control de las cintas que contienen las copias de seguridad y los datos que debe contener y, consecuentemente, hacer el ajuste para que se ajuste a la realidad de la actividad.

En relación con la restauración de copias de seguridad, se evidenció que efectúan restauraciones de copias de seguridad, principalmente, según demanda de usuarios, para lo cual se utiliza el formato de "Solicitud de Restauración de Backup", código FO-TI-185. De acuerdo con lo especificado en el numeral "*9.8 Proceso de Verificación de las Copias de Seguridad*" del manual MG-TI-16, "[…]*, al azar y esporádicamente se realizarán al menos dos (2) pruebas mensuales de restauración de las mismas, en ambientes de trabajo de pruebas*", pero también se indica que "[…] *todas las solicitudes de usuario para la restauración de copias de seguridad, se considerarán una prueba de verificación*". Así que se cumpliría este requisito.

No obstante, las solicitudes o la selección al azar no garantizan que se logre efectuar pruebas de restauración de copias de todos los recursos a los que se les realiza copia (bases de datos, archivos o recursos compartidos, servidores, aplicaciones, repositorios de código fuente), por lo cual se recomienda evaluar la posibilidad de establecer una programación de restauración de copias de seguridad para asegurar que en cada año se incluyan, al menos una vez, una prueba de restauración de cada recurso.

Adicionalmente, está indicado en el Manual, también en el numeral "*9.8 Proceso de Verificación de las Copias de Seguridad*", que "*En todo caso, cualquiera de las tareas de restauración deberá ser registrada en el formato Bitácora de Control de Restauraciones de Copias de Seguridad (FO-TI-24)*". Sin embargo, se verificó en el Listado Maestro de Documentos que el formato FO-TI-24 está derogado desde el 13/10/2017. Al indagar con el administrador/operador de copias de seguridad, éste indicó que el historial de restauraciones y sus resultados quedan almacenados en la herramienta de copias de seguridad.

Tomando en cuenta la mención explícita, en el Manual, de la utilización de formato FO-TI-24 (Bitácora de Control de Restauraciones de Copias de Seguridad) y que éste no se use porque no

está vigente, se configuraría un hallazgo. Pero, dado que la herramienta lleva el control de las copias restauradas y que el citado manual está en actualización, se efectúa una recomendación en el sentido de tener en cuenta la eliminación de la referencia al formato y registrar, de ser el caso, la forma en la que se lleva el control de la restauración las copias de seguridad, identificando, en la medida de lo posible, si fueron a solicitud o las seleccionadas o definidas al azar por el administrador del centro de cómputo.

Por último, se verificó si, de acuerdo con lo especificado en los numerales "*1.1.6.14 Guardar log*" y "*1.2.1.11 Exportar logs*" del Procedimiento Generación de Copias de Seguridad, código PR-TI-11, versión 1.0, se genera copia de respaldo de los resultados arrojados por la herramienta de generación de copias, con el fin de conservar la evidencia de realización de las tareas ejecutadas, o de los archivos de registros automáticos de eventos de la herramienta de *backup*, como evidencia de la adecuada gestión del proceso, y si dichos registros de eventos se conservan en el área de administración de copias según las disposiciones de conservación de registros vigentes.

Se encontró que, si bien la herramienta mantiene los resultados de la ejecución de copias, no se evidenció la generación de copias de respaldo de los resultados arrojados por la herramienta utilizada para esta tarea, es decir, de los *logs* de generación de copias de seguridad. Por lo cual se generó el hallazgo titulado "Ausencia de copias de seguridad de los *logs* generados por la herramienta de generación de copias de seguridad".

Actividad N.° 8 "Continuidad de servicios de TI (Recuperación ante desastres)"

La revisión de esta actividad crítica se circunscribió a la verificación de la operación de la estrategia de recuperación ante desastres de los servicios de TI y seguridad de la información.

El proceso cuenta, entre otros, con los siguientes documentos relacionados con la gestión de copias de respaldo:

Tabla N° 3. Documentación asociada a la Continuidad de servicios de TI (Recuperación ante desastres)

Nombre	Tipo de Documento	Código	Versión	Fecha
Plan de Recuperación ante Desastres	Plan	PL-TI-01	2	31/10/2019
Gestión de Continuidad de Servicios de TI	Procedimiento	PR-TI-20	2.0	10/08/2018
Restauración de la Aplicación Valoricemos	Instructivo	IN-TI-03	2.0	30/05/2018
Restauración Aplicaciones Botón Azul	Instructivo	IN-TI-23	2	20/12/2018
Restauración Sistemas Basados en ODOO	Instructivo	IN-TI-24	2	20/12/2018
Restauración Sistema ORFEO	Instructivo	IN-TI-25	1.0	27/12/2017
Restauración Sistema KACTUS	Instructivo	IN-TI-26	2	20/12/2018
Restauración Sistema STONE	Instructivo	IN-TI-27	2	20/12/2018

Fuente: Intranet, Mapa de Procesos. **Elaboración:** Equipo Auditor.

Mediante entrevistas con funcionarios y colaboradores de la Subdirección Técnica de Recursos Tecnológicos (STRT) y revisión de soportes, se verificó que dicha dependencia tiene establecida una estrategia de recuperación de los servicios de TI ante la ocurrencia de desastres.

Como criterio principal para realizar la respectiva verificación se tomó el Plan de Recuperación ante Desastres, código PL-TI-01, V 2, aunque también se revisaron algunos aspectos del procedimiento e instructivos mencionados en la tabla anterior.

Se evidenció que, en el numeral "*3. ALCANCE*" del citado Plan, está señalado que "[…] *Este plan incluye las actividades necesarias que deberá realizar el equipo de trabajo de la STRT para activación del DRP en caso de que se presente una indisponibilidad tecnológica y física de la sede principal Calle 22 del Instituto de Desarrollo Urbano, es así que su activación, iniciará con el traslado del personal al piso 5 de la sede calle 20 del IDU en los puestos designados de acuerdo con el listado anexo a este documento*." (Subrayado fuera del texto original).

Sin embargo, dentro del Plan el único anexo es el "*9 ANEXO 1. REPORTE DE NOVEDADES*" que corresponde a un formato en el que se registran " […] *los hechos sucedidos que no hayan sido contemplados en el Plan de Recuperación Ante Desastres y las acciones tomadas durante el evento de interrupción,* […]".

Se verificó que el listado referido en el alcance corresponde al archivo de Word titulado "***EQUIPO OPERATIVO MÍNIMO DURANTE LA ACTIVACIÓN DEL DRP***", el cual está identificado, igualmente, como "*ANEXO N°. 1 DEL PLAN DE RECUPERACIÓN ANTE DESASTRES*" y contiene un listado de las personas que conforman el equipo de trabajo de la STRT (principales y suplentes) para activación del DRP y ejercen los roles de "Líder de Mesa de Ayuda", "Mesa de Servicios", "Administrador de Base de datos", "Telecomunicaciones", "Operador Data Center", "Orfeo", "Botón Azul", "Stone", "Página Web", "Aranda", "SIGIDU". De acuerdo con la explicación de los colaboradores entrevistados, la razón por la cual el listado no quedó incluido en el Plan publicado es porque contiene datos como nombres, número de celular y correo electrónico de los colaboradores que forman parte del equipo. Así las cosas, el listado sería únicamente de consulta interna de la STRT.

Tomando en cuenta esta situación y la razón esgrimida, se sugiere ajustar el alcance del documento de manera que se indique, si es necesario, la existencia del equipo operativo mínimo durante la activación del DRP, o del listado de personas que lo conforman, pero retirando la referencia a que el listado está anexo al Plan PL-TI-01.

Así mismo, dado que el listado, en el encabezado, figura como si fuera parte del Plan, como se ve en la imagen N° 3, se recomienda retirarlo como anexo del mismo eliminando el encabezado, o renumerarlo como Anexo N° 2, ya que el anexo 1 es el Reporte de Novedades.

Imagen N° 3. Encabezado del listado del "Equipo Operativo Mínimo Durante la Activación del DRP"

Fuente: STRT.

Es importante mencionar que no hay una directriz de revisión y actualización para este listado, por lo cual se recomienda establecerla y documentarla, de manera que se asegure que el personal registrado está vinculado al IDU y que sus datos son los correctos.

Como parte de la revisión de los documentos mencionados en la Tabla N° 3 se encontró desactualización en los numerales "*4. MARCO NORMATIVO*" del Plan de Recuperación ante Desastres PL-TI-01, versión 2, "*1.3 MARCO NORMATIVO*" del procedimiento PR-TI-20 "Gestión de

Continuidad de Servicios de TI" y de los instructivos de restauración de Valoricemos, Botón Azul, Odoo, Orfeo, Kactus y Stone, como sigue:

a. Plan PL-TI-01
   - Citan la "*Resolución Interna 6315 de 2016, "Por la cual se modifica y actualiza el Sistema de Coordinación Interna del IDU […]"*", la cual fue derogada por la Resolución IDU 2275 de 2018 (junio 1), derogada a su vez por la Resolución IDU 5014 de 2018 (diciembre 20).

   - También, citan la Resolución 305 de 20 de octubre de 2008 "*Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre*" la cual fue modificada por la Resolución 004 de 2017 (noviembre 28) de la Comisión Distrital de Sistemas (CDS). Sin embargo, esta resolución no está incluida.

   - El Plan no relaciona la Resolución 1909 de 2019 (mayo 14), "*Por medio de la cual se define la política MIPG-SIG-IDU, se determinan las directrices y objetivos de los Subsistemas de Gestión, y se adopta la versión 4.0 del Manual de Procesos del IDU*". Esta resolución es importante toda vez que en sus artículos 12 y 13 adopta la Directriz del Subsistema de Gestión de Continuidad del Negocio (SGCN) y establece los respectivos objetivos.

b. Procedimiento PR-TI-20

   - Citan el Decreto 652 de 2011 de la Alcaldía Mayor de Bogotá "*Por medio del cual se adopta la Norma Técnica Distrital del Sistema Integrado de Gestión para las Entidades y Organismos Distritales*", el cual fue derogado por el artículo 14 del Decreto Distrital 591 de 2018.

   - Citan la "*Resolución 447 de 2012 del Instituto de Desarrollo Urbano: "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 fue derogada por la Resolución IDU 852 de 2019 (marzo 8), derogada a su vez por la Resolución IDU 1641 de 2019 (abril 26).

   - Citan la "*Resolución 6315 de 2016 del Instituto de Desarrollo Urbano: "Por la cual se modifica y actualiza el Sistema de Coordinación Interna del IDU, y se deroga la Resolución IDU 22477 de 2014 y sus modificaciones"*", la cual fue derogada por la Resolución IDU 2275 de 2018 (junio 1), derogada a su vez por la Resolución IDU 5014 de 2018 (diciembre 20).

   - No está relacionada la Resolución 1909 de 2019, "*por la cual se define la Política MIPG-SIG-IDU, se determinan las directrices y objetivos de los Subsistemas de Gestión, y se adopta la versión 4.0 del Manual de Procesos del IDU*".

c. Instructivos IN-TI-03, IN-TI-23, IN-TI-24, IN-TI-25, IN-TI-26 e IN-TI-27

   - Relacionan la *Norma Técnica NTC GP-1.000, Calidad en la gestión pública*, la cual no está vigente, tomando en cuenta que fue reemplazada por el modelo Integrado de Planeación y Gestión - MIPG (Decreto 1499/2017 y que fue adoptado en el Instituto con la Resolución 852 de 2019 (marzo 8), actualmente derogada por la Resolución IDU 1641 de 2019 (abril 26).

- Citan la Resolución 305 de 20 de octubre de 2008 "*Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre*" la cual fue modificada por la Resolución 004 de 2017 (noviembre 28) de la Comisión Distrital de Sistemas (CDS). Sin embargo, esta resolución no está incluida.

- Citan la "*Resolución 447 de 2012 del Instituto de Desarrollo Urbano: "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 fue derogada por la Resolución IDU 852 de 2019 (marzo 8), derogada a su vez por la Resolución IDU 1641 de 2019 (abril 26).

Se genera, entonces el hallazgo "Desactualización en el marco normativo de la documentación asociada a la estrategia de recuperación de desastres de TI", toda vez que según el Procedimiento Gestión de la Información Documentada, código PR-AC-07, es responsabilidad del líder de proceso o del líder operativo garantizar que la documentación de un proceso sea adecuada, pertinente y actual.

Se verificó, de acuerdo con lo establecido en el numeral "*5.1 POLÍTICAS OPERACIONALES*" del Plan de Recuperación ante Desastres, cuarta viñeta, que el formato FO-TI-26 "Árbol de Llamadas para DRP" está diligenciado. Sin embargo, se encuentran vacíos en los lugares correspondientes al NIVEL OPERATIVO 2. De acuerdo con indicado por el personal de la STRT, no se diligenció porque la capacidad operativa de la dependencia (cantidad de personal) no es suficiente para cubrir este nivel. Por lo tanto se recomienda verificar la pertinencia de incluirlo, toda vez que pareciera estar diligenciado de manera incompleta, o efectuar la aclaración de por qué no se ha diligenciado.

Es de anotar que no hay una directriz de revisión y actualización para este árbol, por lo cual se recomienda establecerla y documentarla, de manera que se asegure que el personal registrado está vinculado al IDU y que sus datos son los correctos.

Se verificó que en 2019 efectuaron dos pruebas del Plan de Recuperación ante Desastres (DRP), en los meses de marzo y septiembre, las cuales fueron consideradas exitosas, toda vez que lograron recuperar en el tiempo estipulado de 4 horas, de acuerdo con los tiempos de recuperación objetiva (RTO) establecidos por el Instituto.

Ahora bien, en el documento PL-TI-01 está establecido, en el numeral "*5.1 POLÍTICAS OPERACIONALES*", quinta y sexta viñetas que "*Todo el personal de los distintos grupos funcionales de la Subdirección Técnica de Recursos Tecnológicos, deberá estar informado de las responsabilidades que le competen al momento de la activación del DRP, mediante labores de formación, divulgación y prueba de este Plan*" y que "*La efectividad del DRP, será medida mediante pruebas periódicas, según las decisiones y objetivos de medición que sean considerados por parte de la Subdirección Técnica de Recursos Tecnológicos o sus superiores, en los términos y plazos fijados por ellos*."

De acuerdo con estas dos políticas la STRT indicó que las labores de formación, divulgación y prueba de este Plan se desarrollaron mediante reuniones de seguimiento que se efectuaron cada 15 días (o, en ocasiones, por demanda), con la coordinación de la SGGC y la DTAF. En ellas se informaba al equipo las respectivas responsabilidades frente al DRP. Así mismo, el personal participó en las pruebas, según los equipos conformados y niveles o roles establecidos.

Se indagó sobre a qué se referían, con precisión, los términos 'formación' y 'divulgación', toda vez que no es claro si es formación en el mismo DRP o técnica relacionada con conocimientos aplicables, o si la divulgación es del mismo Plan a través de, por ejemplo, la publicación del mismo en los medios institucionales o de si se refiere a divulgar cuándo se realizarían las pruebas, se recomienda especificar a qué se refiere cada una de esas actividades.

Así mismo se determinó que no está claramente especificada cuál sería la periodicidad de las pruebas del DRP, puesto que no se menciona si es mensual, semestral, anual, una vez al año, bianual, etc. Por tanto, se recomienda especificar la periodicidad o frecuencia real en la que se deberían efectuar pruebas al DRP.

El Instituto, como parte de la estrategia de DRP de los servicios de TI cuenta con una solución en la nube. Como parte de las responsabilidades de los operadores del *Data Center* (centro de cómputo) está la de verificar que los componentes de esa solución operen con normalidad. Se comprobó que a través de las herramientas de monitoreo con que cuenta la STRT y de las facilidades o técnicas como *Mirror* para las bases de datos (BD) SQL Server y *Data Guard* para las BD Oracle, se proporciona una infraestructura para mantener bases de datos 'de reserva' sincronizadas con las originales, que aseguran protección de los datos contra fallas, desastres, errores y daños. La sincronización con *Mirror* es en línea y con *Data Guard* se hace cada 20 minutos.

En el numeral 5.2.5 del PL-TI-01 se relacionan las roles y responsabilidades del Equipo de Gestión de Aplicaciones (Nivel Operativo Dos). Dentro de dichas responsabilidades está la de "*Poner en funcionamiento las aplicaciones críticas dentro del RTO definido en el Análisis de Impacto al Negocio – BIA, mediante la aplicación de las soluciones que se necesiten*". Se indagó con uno de los responsables de la administración del sistema Stone si conocía el BIA y el RTO (tiempo máximo de recuperación) que está fijado en 4 horas y se determinó que tenía confusión entre el RTO y el RPO (punto objetivo de recuperación) que corresponde a la máxima tolerancia de pérdida de información definida por los procedimientos críticos y es de 1 día (Fuente: "Informe Análisis de Impacto del Negocio – BIA", código DU-PE-12, versión 1). Así mismo, se encontró que no conoce el BIA. Es de aclarar que se determinó que el BIA no está publicado en la Intranet.

Por lo cual se recomienda a la STRT coordinar con la SGGC y con la Oficina Asesora de Planeación para reforzar los conceptos y/o brindar capacitación u orientación a los participantes del DRP sobre los documentos y aspectos relacionados.

En el numeral 5.2.6 del PL-TI-01 se relacionan las roles y responsabilidades del Equipo Gestión de Mesa de Servicio (Nivel Operativo Dos). Sin embargo, personal de la STRT manifestó (como se mencionó en lo relacionado con el Árbol de Llamadas) que este nivel no está definido debido a que la capacidad operativa actual de la STRT no es suficiente. Por lo tanto se recomienda verificar quién efectuaría estas actividades.

Es importante mencionar que el alcance del Subsistema de Gestión de la Continuidad del Negocio está definido "*para los procesos de adquisición predial, Gestión Contractual, Gestión de las Tecnologías de Información y Comunicación, Gestión Documental y Gestión Financiera, para las sedes Calle 22 y Calle 17*" (Numeral 8.8.3 Alcance, MG-AC-01 Manual MIPG-SIG). Sin embargo, dentro de la documentación relacionada con el DRP para la aplicaciones, relacionan el instructivo de restauración de Valoricemos. Dado que el proceso de Gestión de la Valorización y Financiación no está incluido dentro del alcance del SGCN, se recomienda conciliar con la documentación del SGCN para

determinar si es pertinente que la restauración de Valoricemos forme parte de la estrategia de DRP de servicios de TI.

Por otra parte, en el alcance (numeral 1.2) del Procedimiento Gestión de Continuidad de Servicios de TI, PR-TI-20, versión 2, hablan del Plan de Continuidad de servicios de TI. Se recomienda ajustar el nombre, dado que dicho Plan fue reemplazado por el Plan de Recuperación ante Desastres, PL-TI-01.

En este mismo procedimiento señalan, en el numeral "*1.4. TÉRMINOS Y DEFINICIONES*", que "*Los términos y definiciones aplicables al procedimiento pueden ser consultados en el micro sitio Direccionario* (sic) *de términos IDU HTTPS://WWW.IDU.GOV.CO/PAGE/TRANSPARENCIA/INFORMACION-DEINTERES/GLOSARIO*"; sin embargo, éstos no se encuentran en la página citada.

Por último, el numeral "*1.6.1. Inicio por orden del líder del DRP*" del procedimiento PR-TI-20 establece que "*El procedimiento inicia cuando el líder del DRP, por cuenta propia o por instrucciones del líder del Plan de Continuidad del Negocio, dé la orden para realizar la recuperación de los servicios de TI afectados por la situación de emergencia*". Sin embargo, no está claramente identificados o establecidos criterios que permitan determinar cuando algún incidente o evento puedan clasificarse como situación de emergencia que dé lugar a la recuperación de los servicios de TI afectados o al inicio del DRP.

Por ejemplo, de acuerdo con las matrices de riesgos del proceso, en 2019 se evidenció la materialización de algunos riesgos asociados a la disponibilidad de servicios de TI (reporte efectuado por la STRT corte a 30/04/2019, e identificado en la auditoría al Sistema Integrado de Gestión). No obstante, esta indisponibilidad no fue catalogada como una situación que ameritara activar el DRP, según lo explicado por la STRT porque los tiempos estimados de recuperación eran similares al RTO. No obstante, no se encontró documentación que así lo indique.

Por tanto, se recomienda identificar y/o establecer criterios que permitan determinar cuando algún incidente o evento pueda clasificarse como situación de emergencia que dé lugar a la recuperación de los servicios de TI afectados o al inicio del DRP.

Actividad N.° 9. "Seguimiento a la Gestión"

Dentro de las labores incluidas en esta actividad crítica están la de "[…]. *Analizar y proyectar las estrategias de operación que son requeridas para dar cumplimiento a los servicios de TI, tomando como base los resultados e interpretación del comportamiento de los riesgos identificados,* […]". Así mismo, uno de los insumos para esta actividad corresponde a las matrices de riesgos. De acuerdo con esto, se efectuó una revisión general de los riesgos de gestión del proceso contenidos en la matriz publicada en la intranet, corte 31/08/2019, y que se listan en la siguiente tabla:

Tabla N° 4. Riesgos de gestión del proceso de Gestión de Tecnologías de la Información y la Comunicación

Procedimiento / actividad / producto	Cód.	Riesgo (amenaza)
Desarrollo de Aplicaciones	G.TI.01	Inadecuada definición de los requerimientos del software a desarrollar
Direccionamiento estratégico de TIC	G.TI.02	Insuficiente asignación de recursos para el cumplimiento de los objetivos o actividades requeridas al proceso
Gestión de Infraestructura de T.I.	G.TI.03	Inadecuada gestión de la Infraestructura de TI

Procedimiento / actividad / producto	Cód.	Riesgo (amenaza)
Gestión de Servicios de TI	G.TI.04	Problemas en la relación entre usuarios finales y prestadores de los servicios de T.I.
Seguridad	I.TI.01	Acceso a la información por personas no autorizadas
Seguridad	R.TI.07	Alteración de la configuración de los elementos usados para la prestación de servicios
Seguridad	I.TI.02	Corrupción de software o degradación de aplicaciones
Seguridad	I.TI.03	Daño a los equipos de cómputo de usuario y/o a los archivos contenidos en ellos
Apoyo a la gestión y Seguridad	R.TI.10	Degradación de la calidad o legibilidad de la información almacenada
Seguridad	R.TI.11	Denegación de los servicios de TI
Seguridad	I.TI.04	Explotación de debilidad conocida sobre los componentes tecnológicos y los sistemas de seguridad perimetral
Seguridad	R.TI.13	Incumplimiento de los acuerdos de nivel de servicios en los términos pactados
Gestión	R.TI.14	Lentitud en la respuesta de los servicios de red interna o externa
Seguridad	I.TI.05	Mal uso de los servicios de correo electrónico
Seguridad	R.TI.16	Manipulación de equipo de cómputo de usuario por familiar o tercero sin autorización o sin supervisión
Seguridad	I.TI.06	Afectación a la seguridad de la información durante un evento crítico
Seguridad	I.TI.07	No remover todos los datos y/o aplicaciones de software cuando se devuelven los equipos
Seguridad	I.TI.08	Pérdida o interrupción del servicio de aire acondicionado en el *datacenter*

Fuente: Intranet, Matriz de Riesgos de Gestión, Corte 30/09/2019. **Elaboración:** Equipo Auditor.

Es importante aclarar que a la citada fecha de corte, los riesgos de seguridad de la información y los de gestión se incluían en la misma matriz (formato “Matriz de Riesgos”, código FO-PE-06). No obstante, a la fecha de verificación de la información con el proceso (03/12/2019), en la entidad se estaban adelantando tareas de revisión y actualización de las matrices de riesgos del Instituto, lo cual incluía la separación de los riesgos de seguridad de la información en una nueva matriz. El plazo para que las diferentes dependencias entreguen la actualización mencionada es el 06/12/2019.

Se observó que el formato MATRIZ DE RIESGOS utilizado por la STRT para presentar los riesgos de gestión (FO-PE-05, versión 5) no era el vigente para el periodo reportado, esto tomando en cuenta que en el campo “FECHA DE SEGUIMIENTO” aparece el valor “*4-sep-19*”. El formato vigente al momento del monitoreo/reporte que el área hizo de los riesgos de gestión, periodo mayo - agosto 2019, era el FO-PE-05, versión 6, que fue publicado el 05/06/2019 y derogado el 10/09/2019, según el sistema SUÉ: Información Documentada.

Como consecuencia de lo anterior, la valoración presentada de algunos de los riesgos no corresponde con la establecida en el Manual de Administración del Riesgo, MG-PE-18, versión 9 (publicado el 04/06/2019). Por ejemplo, en la matriz revisada se encontraron 11 riesgos calificados, en el riesgo residual, con el valor “*INFERIOR*” (G.TI.03, G.TI.04, I.TI.01, I.TI.02, I.TI.03, R.TI.10, R.TI.14, I.TI.05, R.TI.16, I.TI.06, I.TI.07, e I.TI.08) y con probabilidad “*Remota*” 15 (los anteriores, exceptuando el I.TI.07, y los riesgos G.TI.02, R.TI.07, R.TI.11, e I.TI.04).

En el manual MG-PE-18, versión 9 está establecido que las opciones para calificar la probabilidad son "*Casi Segura*", "*Alta*", "*Posible*", "*Baja*" o "*Rara vez*" y las opciones para calificar el impacto son "*Catastrófico*", "*Mayor*", "*Moderado*", "*Menor*" o "*Insignificante*". La combinación de probabilidad e

impacto daría como resultado la calificación del riesgo con alguna de las opciones "*Extremo*", "Alto", "*Moderado*" o "*Bajo*".

Dado lo anterior, se recomienda verificar, cada que se vaya a efectuar el monitoreo y/o actualización de los riesgos, la utilización de formatos vigentes, con el fin de que la calificación de probabilidad, impacto, riesgo inherente y riesgo residual esté acorde con las directrices respectivas.

De acuerdo con lo consignado en la matriz de riesgos del proceso analizada y dado que está en actualización, no se efectuó un análisis exhaustivo de cada uno de los controles, sino se revisaron aspectos generales.

Se observó que los controles establecidos buscan mitigar los riesgos. Sin embargo, se identificaron algunos aspectos a mejorar, que se enuncian a continuación y que aplican para todos los riesgos:

1. Definición del responsable

En la matriz de riesgos del proceso se observó que los responsables de llevar a cabo la ejecución de los controles, en todos los casos, corresponde a "Profesional Especializado". Sin embargo, estos no corresponden a cargos o perfiles de personas responsables de ejecutar los controles, es decir, no se identifica qué cargo o rol específico ejecuta cada control.

Es importante aclarar que el responsable de ejecutar los controles es, de acuerdo con lo indicado en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - Riesgos de Gestión, Corrupción y Seguridad Digital, versión 4, del Departamento Administrativo de la Función Pública, una persona con la autoridad, competencia y conocimientos pertinentes para hacerlo, de acuerdo con el objetivo y alcance del proceso, por lo cual se recomienda que se revisen los responsables y se registren en la matriz, para cada uno de los controles, los roles, perfiles y/o cargos de quien los ejecuta.

Se recomienda identificar y especificar en la redacción de cada control quién es el responsable de la materialización.

2. Periodicidad de ejecución

No se evidenció, en la matriz de riesgos del proceso, la periodicidad para ejecución de los controles (diaria, quincenal, mensual, según evento etc.), aunque en algunos casos, en la misma redacción del control se especifica una periodicidad, por ejemplo, en el control "*5. Seguimiento semanal de avance*

3. Propósito del control

En general no se evidenció, en su redacción, cuál es el propósito de los controles. Por ejemplo:

- No se registra el objeto del control "*Cláusulas de confidencialidad en los contratos con terceros*" identificado para el riesgo G.TI.03 "*Inadecuada gestión de la Infraestructura de TI*.

- En el caso del riesgo R.TI.10 "*Degradación de la calidad o legibilidad de la información almacenada*" se observó que el control "*El acceso a la información y servicios institucionales debe hacerse mediante*

la autenticación de los usuarios en la red de datos en el Directorio Activo, en donde se cuenta con la política de gestión de contraseñas" no registra el propósito o cómo ayuda a mitigar el riesgo o eliminar/atacar alguna de las causas identificadas.

En general, se recomienda evaluar la construcción y pertinencia de los controles, teniendo en cuenta que éstos deben tener un propósito que indique para qué se realizan y deben llevar a prevenir las causas que generan el riesgo o a detectar su materialización.

En algunos casos está relacionados procedimientos completos como controles, sin embargo es recomendable verificar si todas las actividades relacionadas en los procedimientos aplican para mitigar/eliminar/atacar las causas del riesgo. Tal es el caso del riesgo G.TI.03 que tiene asociado el control "*Procedimientos PR-TI-17 y PR-TI-23 Gestión de servidores y Gestión de telecomunicaciones*".

Es necesario mencionar que en la matriz no es posible identificar con claridad la asociación de controles con causas, es decir cuál(es) control(es) apuntan a atacar cada una de las causas identificadas. Además, en el ejercicio se identificaron algunos riesgos para los cuales, no todas las causas tienen controles; por ejemplo, en el riesgo G.TI.03, la causa "*3 Bajo nivel de control en la generación y restauración de copias de seguridad*" no tiene asociado ningún control y en el riesgo R.TI.10 sucede lo mismo con la causa "*6 Tablas de retención documental desactualizadas o no aplicadas*".

Por lo tanto, se recomienda que se identifique, para cada causa, cuáles son sus controles, tomando en cuenta que para cada una debe existir, mínimo, un control.

Materialización de Riesgos

En la matriz con corte a 31/08/2019, la STRT reportó la materialización del riesgo R.TI.13 "*Incumplimiento de los acuerdos de nivel de servicios en los términos pactados*" debido a que "*En el periodo evaluado se presentaron casos que fueron cerrados fuera de los tiempos de los acuerdos de nivel de servicio, los que están siendo verificados*." El periodo evaluado es el comprendido entre el 01/05/2019 y el 31/08/2019.

Se verificó que la STRT presentó, con memorando 20195360323823 del 27/09/2019 un plan de mejoramiento que incluía acciones relacionadas con la materialización de los riesgos identificados en la auditoría SIG por indisponibilidad de servicios de TI (riesgos G.TI.03, R.TI.07, y R.TI.11) y el riesgo R.TI.13, por incumplimiento de los acuerdos de nivel de servicios.

Las acciones planteadas para la materialización del último son:

Tabla N° 5. Acciones de mejora planteadas para la materialización del riesgo R.TI.13

Código Acción	Acción
Accion_1910	Divulgación y sensibilización de la matriz de riesgos del proceso
Accion_1911	Sensibilización en el manejo de ARANDA
Accion_1912	Configurar notificaciones de asignación y avance en ARANDA.

Fuente: CHIE: Plan Mejoramiento Institucional

Riesgos de Corrupción

La Oficina de Control Interno realizó seguimiento a la matriz de riesgos de corrupción del proceso, con corte al 31/08/2019, y en dicho proceso se evaluaron la ejecución de las actividades y operaciones asociadas a los controles. El resultado y recomendaciones se presentan detalladamente en el anexo Análisis Matriz Riesgos de Corrupción. No obstante, es de resaltar que las situaciones identificadas son similares a las descritas para los riesgos de gestión en cuanto a la utilización del formato vigente, los propósitos de los controles, la frecuencia de aplicación, las evidencias y la asociación de controles a las causas, entre otras.

Actividad N.° 10 "Optimización del proceso"

La revisión del estado de las acciones de mejoramiento se realizó mediante consulta en el aplicativo CHIE: Plan Mejoramiento Institucional, para 8 acciones que se encontraban en estado "*Terminado*", pero no "*Cerrado*". A continuación, se presentan los resultados de la evaluación de efectividad, de las acciones analizadas:

Tabla N° 6. Evaluación de efectividad de acciones de planes de mejoramiento

Acción	Nombre Hallazgo	Acciones propuestas	Evaluación de efectividad
1292	No aplicación del procedimiento PR-TI-20 GESTIÓN DE CONTINUIDAD DE SERVICIOS DE TI, versión 1.0	Actualizar y gestionar la aprobación del procedimiento PR-TI-20 GESTIÓN DE CONTINUIDAD DE SERVICIOS DE TI. Fecha fin: 14/08/2018	Como quedó consignado para la terminación de esta acción, el procedimiento fue actualizado a la versión 2, simplificándolo. Como se observa en el desarrollo del presente informe de auditoría al proceso de Gestión de TIC, el proceso se relaciona directamente con la aplicación del Plan de Recuperación ante Desastres DRP. Por lo tanto se determina como efectiva la acción y se cierra.
1293		Crear una primera versión del documento plan de recuperación de desastres -DRP- (para los servicios de TI) y gestionar su aprobación. Fecha fin: 30/08/2018	Como quedó consignado para la terminación de esta acción, Se evidenció la creación y publicación en el Mapa de Procesos del Instituto, en la Intranet, del "Plan de recuperación ante desastres", código PL-TI-01, versión 1.0. Como se observa en el desarrollo del presente informe de auditoría, el Plan de Recuperación ante Desastres fue probado en dos oportunidades y ya se encuentra en su versión 2 Por lo tanto se determina que la acción fue efectiva y se cerrará.
1294		Crear el plan de pruebas para el DRP y ejecutarlo al menos una vez en la vigencia actual Fecha fin: 10/12/2018	Se evidenció la realización de dos pruebas al DRP, por lo tanto se determina que la acción fue efectiva y se cerrará. Se recomienda efectuar pruebas por lo menos una vez cada año.
1295	No han efectuado pruebas para la restauración del aplicativo Valoricemos	Actualizar el instructivo IN-TI-03 RESTAURACIÓN DE LA APLICACIÓN VALORICEMOS V 1.0 e incluirlo en el calendario de pruebas de los aplicativos de TI mencionada en el H/1. Fecha fin: 30/05/2018	El 30 de mayo de 2018 se actualizó el documento "Instructivo de restauración de la aplicación Valoricemos" a la versión 2.0 Se evidenció la realización de una prueba de escritorio de la restauración de la aplicación Valoricemos, en julio de 2018, que concluyó que "*En la actualidad se cuenta con un plan debidamente estructurado para la recuperación de los diferentes elementos del sistema de información VALORICEMOS ante una posible catástrofe que interrumpa la disponibilidad del servicio. Se realizan ajustes a las instrucciones para mejor comprensión y mayor claridad para el usuario lector-ejecutor y se adicionan secciones relacionadas con el alistamiento de la máquina de usuario final o cliente para que el documento se enfoque sólo en su objetivo principal*".

Acción	Nombre Hallazgo	Acciones propuestas	Evaluación de efectividad
			Por lo tanto, se considera efectiva la acción y se cerrará. Se recomienda efectuar pruebas de restauración de la aplicación en ambiente de pruebas.
1501	NC 1: Incumplimiento de actividades establecidas en el Manual de Copias de Seguridad	Hacer reuniones bimestrales con el área encargada del contrato de almacenamiento y custodia de los medios magnéticos en sitio externo. Fecha fin: 28/12/2018	Se verificó la realización de reuniones en los meses de marzo, junio, agosto y septiembre de 2019. Si bien, la periodicidad no ha sido en todos los casos, bimestral, como lo indicaba la acción, se observa que la STRT ha cumplido con esta obligación establecida en el Manual MG-TI-16 de verificación al supervisor del contrato de almacenamiento y custodia externa de medios magnéticos. Por tanto, se considera efectiva y se cerrará. Se recomienda tener presente esta obligación y, de ser posible, efectuar una visita a las instalaciones del contratista para comprobar la aplicación de las condiciones pactadas en el contrato en relación con las condiciones de temperatura y almacenaje de los medios magnéticos.
1503		Elaborar informe y presentarlo a la Subdirectora, sobre el estado de los trabajos de copias de seguridad y restauración de acuerdo con la periodicidad indicada en el MG-TI-16 “Manual de Copias de Seguridad”. Fecha fin: 10/09/2019	Se verificó que el encargado ha continuado con la elaboración y presentación, a la Subdirectora de la STRT, del informe sobre el estado de los trabajos de copias de seguridad y restauración de acuerdo con la periodicidad indicada en el MG-TI-16 “Manual de Copias de Seguridad. Por tanto, se considera efectiva y se cerrará.
1504		Elaborar y ejecutar plan de actividades para verificar la restauración de copias de respaldo. Fecha fin: 28/02/2019	Se evidenció la realización de pruebas de restauración por demanda que, según el manual, cuentan dentro de las 2 que deben efectuarse mensualmente. Adicionalmente, la programación de *Backup* se encuentra en la herramienta y se ejecuta según lo programado. Por otra parte, tomando en cuenta que el manual MG-TI-16 está en proceso de actualización, se recomienda verificar si aplica la elaboración de un cronograma ya que la programación se encuentra en la herramienta. Se considera efectiva y se cerrará
1506	NC 3: Inconsistencias en la información del reporte de casos atendidos	Actualizar los documentos: DUTI01 - Catálogo de servicios de tecnologías de la información y la comunicación y PRTI06 – Gestión de servicios de tecnologías de la información, para armonizar con el sistema ARANDA. Fecha fin: 16/11/2018	Para la terminación de la acción, el 02/04/2019, se verificó que el procedimiento "Gestión de Servicios de Tecnologías de la Información", código PR-TI-06, fue actualizado de la versión 2.0 a la 3.0 (publicada el 15/11/2018) y que el "Catálogo de servicios de tecnologías de la información y la comunicación", código DU-TI-01 fue actualizado (el 29/03/2019) de la versión 3.0 a la versión 4.0, indicando en el control de versiones que fueron incluidos "[...] *temas de tiempo de atención y contingencia*". NOTA: Es importante recordar que la acción, en el seguimiento corte 31/12/2018, se dio por no cumplida, por lo cual, se terminó sólo hasta el seguimiento de abril de 2019. Si bien se actualizaron los documentos, en el monitoreo de riesgos de gestión efectuado por la STRT con corte 31/08/2019, la misma dependencia evidenció incumplimiento de los acuerdos de niveles de servicios (ANS). Por esto, se considera inefectiva la acción, dado que la actualización documental no fue suficiente para evitar que se presentara nuevamente el incumplimiento de los ANS y, por ende, las inconsistencias en la información de casos atendidos.

Acción	Nombre Hallazgo	Acciones propuestas	Evaluación de efectividad
			De acuerdo con lo descrito, se da por inefectiva la acción y se cancela. Se aclara que con la presentación del plan de mejoramiento descrito en el aparte de riesgos (memorando 20195360323823 del 27/09/2019) se considera que las tres acciones planteadas suplirían la acción cancelada.

Fuente: Aplicativo CHIE: Plan Mejoramiento Institucional. **Elaboración**: Equipo Auditor.

En resumen, de las 8 acciones revisadas, se consideraron efectivas 7 y una inefectiva, la cual fue reemplazada por las acciones 1910, 1911 y 1912.

Revisión contractual

1. **Contrato IDU-1520-2018** (Adquisición de software especializado que permita la gestión de permisos, seguimiento a recursos, carpetas y archivos de datos no estructurados).

Este contrato se derivó del proceso de selección identificado como IDU-SASI-DTAF-012-2018, adjudicado mediante Resolución 5591 del 27/11/2018 y fue suscrito coincidente con los documentos de adjudicación el 17/12/2018; cumplidos los requisitos de perfeccionamiento, se firmó el acta de inicio el 27 del mismo mes y año.

En cuanto a su ejecución se evidenció el trámite de la orden de pago 694 del 09/04/2019 y su liquidación mediante acta del 17/05/2019.

Ahora bien, de la revisión legal específica, se derivó el requerimiento al área auditada efectuado mediante correo electrónico del 25/11/2019, en el que se solicitó la siguiente información:

> "*1. Certificación del contratista por medio de la cual acreditó estar al día en el "pago de aportes parafiscales relativos al Sistema de Seguridad Social, así como los propios del SENA, ICBF y Cajas de compensación familiar y demás Impuestos que correspondan, de conformidad con lo dispuesto en la ley".*
> *2. Certificación del contratista "de cumplimiento de las obligaciones laborales y de pago de aportes a la seguridad social y parafiscales, de conformidad con lo señalado por el artículo 50 de la Ley 789 de 2002".*
> *3. Constancia de entrega del Plan de trabajo, donde se establezcan las fechas de entrega del certificado de licenciamiento, documentos que hacen parte del anexo técnico numeral "1.1.19. Documentación" y fechas de implementación, puesta en funcionamiento y transferencia de conocimiento.*
> *4. Constancia de entrega y aprobación del cronograma de trabajo donde se detallen las actividades de pre-implementación, implementación y post-implementación y se relacionen los tiempos de ejecución y personal involucrado por Actividad.*
> *5. Indicar si el IDU ha requerido al contratista algún soporte o instalación de parche. En caso positivo, precisar el protocolo adelantado y la constancia de atención y cierre del evento."*

En consideración a la respuesta recibida mediante correo electrónico del 27/11/2019, se realizó visita *in situ* el 02/12/2019, a efectos de precisar información y contenido en relación con:

- **Plan de trabajo**: se indagó puntualmente sobre la fecha de presentación inicial del mismo, toda vez que el numeral 1, del literal B, de la cláusula 11 Obligaciones del Contratista, señala:

"*Elaborar el plan de trabajo, donde se establezcan las fechas de entrega del certificado de licenciamiento, documentos que hacen parte del anexo técnico numeral "1.1.19. Documentación" y fechas de implementación, puesta en funcionamiento y trasferencia de conocimiento, dentro de los cinco (5) días hábiles siguientes a la firma del Acta de Inicio.",* en el entendido que la misma se suscribió el 27/12/2018. En la visita se puso a disposición una impresión del Plan de Trabajo presentado inicialmente por el contratista, del 28/12/2018, cumpliendo en la presentación con el parámetro inicial.

- **Cronograma**: se solicitó información de contenido y fecha de presentación inicial del mismo, toda vez que el numeral 2, del literal B, de la cláusula 11 Obligaciones del Contratista, señala: "*Establecer un cronograma de trabajo donde se detalle las actividades de pre implementación, implementación y post-implementación donde se relacione los tiempos de ejecución y personal involucrado por Actividad, dentro de los cinco (5) días hábiles siguientes a la firma del Acta de Inicio*", teniendo en cuenta que la misma se suscribió que el 27/12/2018.

Es importante precisar que el MANUAL DE INTERVENTORÍA Y/O SUPERVISIÓN DE CONTRATOS - MG-GC-01 en la parte pertinente del numeral "*6.1 Generalidades*", dispone: *"La interventoría y la supervisión, junto con el equipo de apoyo a la supervisión de los contratos, de acuerdo con la naturaleza propia de las obligaciones/funciones a su cargo, deben exigir la calidad de los bienes, obras y servicios adquiridos en el marco de un contrato estatal, verificando que se cumplan todas las condiciones técnicas, económicas y legales pactadas. Para ello deberán garantizar que se cumplan las disposiciones legales y aquellas normativas internas del IDU, así mismo, deberán promover y verificar el cumplimiento de lo dispuesto en el respectivo contrato."* (Subrayado fuera de texto).

Al respecto, en el caso que nos ocupa, si bien es cierto se puso a disposición del equipo auditor una impresión del cronograma de actividades que en su contenido cumpliría con los ítems descritos en el contrato, no lo es menos que no se acreditó por parte del equipo auditado el cumplimiento de la condición temporal de su presentación, es decir dentro de los cinco (5) días hábiles siguientes a la firma del Acta de Inicio, lo que evidencia debilidades en el ejercicio de la supervisión del contrato, en contravención a la disposición citada del Manual de Interventoría y/o Supervisión de Contratos.

De otra parte, en consideración a que, a pesar de haber consultado el expediente (ORFEO), se hizo necesario requerir información adicional, lo que soporta la recomendación al área auditada para que se incorporen al expediente ORFEO del respectivo contrato, todos los documentos, comunicaciones y soportes de la actividad contractual.

En cuanto a ejecución contractual, se tiene que el contrato IDU-1520-2018 fue liquidado mediante acta del 17/05/2019, la cual fue remitida en la misma fecha a la Dirección Técnica de Gestión Contractual, mediante memorando 20195360112343 para su publicación; sin embargo, consultada la plataforma SECOP II (28/11/2019), el estado del contrato se registra como "*Firmado*" y no se ubica el acta de liquidación citada.

El Decreto 1082 de 2015, en su Artículo 2.2.1.1.1.7.1. *Publicidad en el SECOP*, prevé "*La Entidad Estatal está obligada a publicar en el Secop los Documentos del Proceso y los actos administrativos del Proceso de Contratación, dentro de los tres (3) días siguientes a su expedición".*

En concreto, respecto al acta de liquidación, se ha ocupado el MANUAL DE INTERVENTORÍA Y/O SUPERVISIÓN DE CONTRATOS MG-GC-01 Versión 6.0 en el numeral 9.7.1 Reglas de la Liquidación, así:

"[…]
12. Una vez suscrita el acta de liquidación, la dependencia a cargo del contrato deberá remitirla a la DTGC al día siguiente de su suscripción, para su publicación en los portales de contratación."

Así mismo, esta obligación legal ha sido objeto de diversos pronunciamientos al interior del Instituto, a efectos de ajustar su operatividad a su estructura organización; es así que se han generado instrucciones jurídicas, memorandos y guías, entre los que se pueden citar los memorandos 20125050215243, 20134350150453, 20174350188953, 20194350101733 y 20194350199723.

Si bien es cierto la auditoría se realiza al Proceso de Gestión de las Tecnologías de Información y Comunicación, no es posible desconocer el incumplimiento del deber legal de publicar la actividad contractual del Instituto en el SECOP, referida particularmente, en este caso, a la Dirección Técnica de Gestión Contractual - DTGC como administradora general de las plataformas, tal como lo señala el último memorando citado y teniendo en cuenta que el acta de liquidación le fue remitida oportunamente para su publicación por la STRT.

Por lo anterior, este aspecto debe ser considerado en la construcción del Plan de mejoramiento que se derive de este ejercicio de auditoría, para que con base en el análisis de causas que se realice y las acciones que se establezcan, se definan los responsables de la ejecución de las mismas.

2. **Contrato IDU-1522-2018** (Adquirir una solución de mitigación de ataques de denegación de servicio distribuido anti -DDOS).

Este contrato se derivó del proceso de selección identificado como IDU-SASI-DTAF-013-2018, adjudicado mediante Resolución 5555 del 29/11/2018 y se suscribió coincidente con los documentos de adjudicación el 18/12/2018; cumplidos los requisitos de perfeccionamiento, se firmó el acta de inicio el 26 del mismo mes y año.

En cuanto a su ejecución se evidenció el trámite de la orden de pago 185 del 18/01/2019 y su liquidación mediante acta del 17/05/2019.

Ahora bien, de la revisión legal específica, se derivó el requerimiento al área auditada, mediante correo electrónico del 22/11/2019, en el que se solicitó la siguiente información:

"*1. Certificación del contratista por medio de la cual acreditó estar al día en el "pago de aportes parafiscales relativos al Sistema de Seguridad Social, así como los propios del SENA, ICBF y Cajas de compensación familiar y demás Impuestos que correspondan, de conformidad con lo dispuesto en la ley".*
2. Certificación del contratista "de cumplimiento de las obligaciones laborales y de pago de aportes a la seguridad social y parafiscales, de conformidad con lo señalado por el artículo 50 de la Ley 789 de2002".
3. El plan de trabajo presentado en su oportunidad por el contratista, junto con la constancia de aprobación por parte del supervisor del contrato.
*4. Compromiso del contratista de prestar el servicio de soporte y garantía por tres (3) años, en un esquema 7*24*365*4, debidamente aprobado por el supervisor.*
5. Resultados de la prueba de funcionalidad del esquema de implementación.
6. Soporte de la transferencia específica de conocimiento realizada por el contratista, (incluido material de estudio).
7. Soporte de la garantía de 3 años otorgada por el FABRICANTE.

8. Indicar si se ha requerido por parte del IDU algún mantenimiento correctivo. En caso positivo, precisar el protocolo adelantado y la constancia de atención y cierre del evento."

En consideración a la respuesta recibida mediante correo electrónico del 27/11/2019, se realizó visita *in situ* el 02/12/2019, a efectos de precisar información y contenido en relación con el Plan de trabajo, transferencia de conocimiento y la prueba de funcionalidad.

En la misma fecha y según consta en acta independiente, previamente al requerimiento de información específica, se solicitó al área auditada precisión conceptual respecto a: ¿Qué se entiende por prueba de funcionalidad? ¿Para realizar estas pruebas de funcionalidad está previsto algún protocolo? ¿Cómo se documenta esta prueba de funcionalidad? A estos interrogantes, personal de la STRT dio respuesta en los siguientes términos:

La prueba de funcionalidad "*Es una verificación respecto a que el software o hardware hace lo que se pidió que hiciera*". En cuanto a su documentación fue indicado que para el software de desarrollo interno la dependencia cuenta con procedimientos; sin embargo, tratándose de software o hardware externo no hay un procedimiento documentado, al respecto, "*se ejecutan buenas prácticas de mercado en el sentido de probar que el dispositivo o programa haga lo que debe hacer*". En cuanto al último interrogante, manifiesta el área auditada: "*En el trascurso de la instalación se van realizando pruebas que se documentan incluyendo las constancias en las respectivas actas*".

Obtenida la precisión anterior, frente a la solicitud particular, se continuó la entrevista en relación con aspectos particulares del contrato objeto de revisión, en relación con:

- **Plan de trabajo**: se indagó puntualmente sobre la fecha de presentación inicial del mismo, toda vez que el numeral 1, del literal B, de la cláusula 11 Obligaciones del Contratista, señala: "*Entregar un plan de trabajo, donde se establezcan las fechas de entrega, instalación y configuración de la solución ofertada. El cual debe ser aprobado por el supervisor del contrato, dentro de los dos (2) días hábiles siguientes a la firma del Acta de Inicio*", en el entendido de que la misma se suscribió el 26/12/2018. En la visita manifestó el área auditada "*que dada la coyuntura del inicio de vigencia no se contaba con personal suficiente e idóneo para asignar el apoyo a la supervisión. Esta falencia se subsanó con la ejecución del PAA con la contratación de los PSPs de apoyo especializados en temas de seguridad informática.*"

Respecto a lo manifestado por el área auditada, se precisó que el segundo día hábil siguiente a la suscripción del acta de inicio correspondió al 28/12/2018; adicionalmente, no es de recibo para el equipo auditor que, frente a obligaciones contractuales esgriman argumentos de esta índole, por tanto es pertinente considerar las disposiciones contenidas el numeral 6.1 del MANUAL DE INTERVENTORÍA Y/O SUPERVISIÓN DE CONTRATOS - MG-GC-01 haciendo evidente nuevamente, las debilidades en el ejercicio de la supervisión del contrato.

- **Transferencia de conocimiento:** se solicitó precisar información sobre las horas de trasferencia, así como el tipo de vinculación de quienes asistieron a las jornadas de capacitación, teniendo en cuenta que el numeral 5, del literal B, de la cláusula 11 Obligaciones del Contratista, señala: "*Realizar una transferencia de conocimiento en las instalaciones del IDU, para cuatro (4) funcionarios con una intensidad horaria de mínimo cuarenta (40) horas sobre la configuración y administración de la plataforma implementada. Debe incluir material de estudio*". (Subrayado fuera de texto).

Indagado el equipo auditado sobre el tipo de vinculación de quienes asistieron a las jornadas de capacitación se evidenció que de los 6 asistentes, 3 son funcionarios de planta (Esperanza Valencia, Marco Guerrero y Raúl Rodríguez) y 3 contratistas (Leonardo Espinosa, Wilmar Díaz y Mario Carvajal), con lo que se estaría inobservado la disposición contractual, toda vez que todos las personas capacitadas debían ser de planta.

De otra parte, de los listados de asistencia aportados en la auditoría, se evidenciaron 7 y 1/2 horas de capacitación / transferencia de conocimiento y, en relación con el tiempo restante, aportaron un oficio del contratista del 25/02/2019 (sin radicación ORFEO), cuyo asunto es "*Acta de Compromisos pendientes*", en el que en el numeral 4 se lee: "*Las 32 horas de transferencia de conocimiento pendientes se aplicar* (sic) *como horas de soporte presencial*", indicando como fecha de compromiso "*Se coordinará fecha con la entidad*", sin que se haya aportado a la auditoría constancia de recibo efectivo de este soporte.

Lo anterior evidencia nuevamente debilidades en el ejercicio de la supervisión del contrato, en contravención a lo dispuesto Manual de Interventoría y/o Supervisión de Contratos, código MG-GC-01, numeral "*6.1 Generalidades*", atendiendo la descripción y análisis efectuado para el contrato IDU-1520-2018

- **Prueba de funcionalidad**.- Mediante correo electrónico del 02/12/2019 el equipo auditado manifestó: "[…] *las pruebas funcionales pata este tipo de equipos se hacen durante el proceso de implementación. Adicional, en el plan de trabajo se indicó que el 22 de diciembre se harían las pruebas funcionales. Es así como en el REPORTE DE ACTIVIDADES de fecha 22 de diciembre, se relata que ese día a las 4 p.m. hace la instalación y configuración de equipo*."

Ante lo manifestado por el área, se constataron tanto el plan de trabajo como el reporte de actividades, siendo consistente su contenido.

Como observación general y en consideración a que a pesar de haber consultado el expediente (ORFEO), se hizo necesario requerir información adicional, se reitera la recomendación a la STRT para que se incorporen al expediente ORFEO del respectivo contrato, todos los documentos, comunicaciones y soportes de la actividad contractual.

En cuanto a ejecución contractual, se tiene que el contrato IDU-1522-2018 fue liquidado mediante acta del 17/05/2019, la cual fue remitida en la misma fecha a la Dirección Técnica de Gestión Contractual, mediante memorando 20195360112963 para su publicación. Sin embargo, consultada la plataforma SECOP II (28/11/2019), el estado del contrato se registra como "*Firmado*" y no se ubica el acta de liquidación citada, soportándose nuevamente el hallazgo imputado a la Dirección Técnica de Gestión Contractual - DTGC, relacionado con la ausencia de publicaciones SECOP, que se identificó y describió al evaluar el tema para el contrato IDU-1520-2018.

Por lo anterior, este aspecto debe ser considerado en la construcción del Plan de mejoramiento que se derive de este ejercicio de auditoría, para que con base en el análisis de causas que se realice y las acciones que se establezcan, se definan los responsables de la ejecución de las mismas.

3. **Contrato IDU-PSP-1298-2019** (Prestar servicios profesionales para apoyar los asuntos relacionados con los servicios de tic, para identificar problemas que surjan en los controles de

seguridad establecidos para salvaguardar la confidencialidad, integridad y disponibilidad de la información del Instituto) –LUIS ALBERO CORTÉS CASTIBLANCO

En primer lugar, se verificó la existencia de esta contratación el Plan Anual Adquisiciones (PAA) que se encuentra publicado en el Portal SECOP II, ubicándose el cupo 1232 consistente con el contrato que se evalúa. Al respecto, se recomienda que se incluya, en el expediente digital ORFEO, el soporte impreso del PAA, como un soporte más del proceso de contratación.

Para efectos de la revisión documental, se tuvo en cuenta la información registrada en el SIAC y en el aplicativo ORFEO, expediente 20194351912000127 9E. En primer término, se consultó el formato FO-GC-10 "*Lista de chequeo para la verificación documental de contratación*", que sirve de soporte para el trámite del respectivo contrato; para efectos de la auditoría, se revisó la documentación anexa encontrándose ajustada a las disposiciones legales y reglamentarias que rigen esta modalidad de contratación.

Es importante mencionar, en particular, la revisión efectuada en cuanto el cumplimiento de la Resolución 5876 de 2018 *"Por la cual se establecen los valores de referencia para honorarios de los Contratos de Prestación de Servicios de Apoyo a la Gestión del Instituto de Desarrollo Urbano y se dictan otras disposiciones*", respecto de las condiciones de experiencia, del Formato Único de Hoja de vida incluyendo la declaración de no existencia de inhabilidades e incompatibilidades para contratar.

En cuanto a la ejecución contractual, el equipo auditor revisó los certificados de cumplimiento generados en desarrollo del contrato y, mediante correo electrónico del 20/11/2019, solicitó la siguiente información puntual:

"1. *Memorando remisorio del acta de inicio a la Dirección Técnica de Gestión Contractual - DTGC para su publicación en los portales.*
2. *Memorando remisorio de cada uno de los certificados mensuales de ejecución a DTGC para su publicación en los portales.*
3. *Revisados los informes de ejecución del contrato que se ubicaron en el expediente ORFEO, se requieren los siguientes soportes/productos que respaldan las correspondientes actividades ejecutadas:*
   a. Informe de ejecución ABRIL
      ÍTEM 1: propuesta presentada en su oportunidad por el contratista
      ÍTEM 4: constancia de remisión de la solicitud enunciada
   b. Informe de ejecución MAYO
      ÍTEM 3: constancia de "entrega de avance" de la guía de evidencia Digital enunciada.
   c. Informe de ejecución JUNIO
      ÍTEM 2: constancia de remisión de las listas de chequeo enunciadas.
   d. Informe de ejecución JULIO
      ÍTEM 3: constancia de remisión de la resolución enunciada
   e. Informe de ejecución AGOSTO
      ÍTEM 3: constancia de remisión de la resolución enunciada"

En consideración a la respuesta recibida mediante correo electrónico del 22/11/2019, se concluye el cumplimiento general de las disposiciones sobre la materia por parte de la STRT; sin embargo, se evidencia que a pesar de que la STRT remitió oportunamente a la Dirección Técnica de Gestión Contractual las constancias de ejecución periódica, las mismas fueron publicadas en el SECOP I extemporáneamente, como se enuncia en la siguiente tabla:

Tabla N° 7. Informes de ejecución contrato IDU-PSP-1298-2019

Periodo certificado	Remisión a DTGC	Publicación (corte a 03/12/2019)
Abril (parcial) - Mayo	Correo electrónico 04/06/2019	16/10/2019
Junio	Correo electrónico 05/07/2019	16/10/2019
Julio	Correo electrónico 31/07/2019	16/10/2019
Agosto	Correo electrónico 3/09/2019	16/10/2019
Septiembre	Correo electrónico 30/09/2019	16/10/2019

Fuente: Memorandos STRT-Registros SECOP I - Consolidación equipo auditor

Al respecto es preciso, tener en cuenta lo dispuesto en el **Decreto 1081 de 2015,** "*Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República",* **Artículo 2.1.1.2.1.8 "*Publicación de la ejecución de contratos.*** *Para efectos del cumplimiento de la obligación contenida en el literal g) el del artículo 11 de la Ley 1712 de 2014, relativa a la información sobre la ejecución de contratos, el sujeto obligado debe publicar las aprobaciones, autorizaciones, requerimientos o informes del supervisor o del interventor, que prueben la ejecución del contrato."*

A efectos de dar cumplimiento a la anterior disposición, se generaron los memorandos 20164350100803 20174350188953 y 20194350199723, a través de los cuales se precisaron temas operativos para su cumplimiento.

Si bien es cierto la auditoría se realiza al Proceso de Gestión de las Tecnologías de Información y Comunicación, no es posible desconocer el incumplimiento del deber legal de publicar oportunamente la actividad contractual del Instituto en el SECOP, referida particularmente en este caso, a la DTGC, como administradora general de las plataformas, tal como lo señala el último memorando citado, teniendo como sustento fáctico las fechas de remisión de los informes de ejecución frente a la fecha de publicación efectiva.

Por lo anterior, este aspecto debe ser considerado en la construcción del Plan de mejoramiento que se derive de este ejercicio de auditoría, para que con base en el análisis de causas que se realice y las acciones que se establezcan, se definan los responsables de la ejecución de las mismas.

4. **Contrato IDU-1580-2019** (Contratar el servicio de pruebas de hacking ético a la infraestructura tecnológica e ingeniería social al personal del IDU).

Este contrato se derivó del proceso de selección identificado como IDU-SAMC-DTAF-006-2019, adjudicado mediante Resolución 5849 del 23/09/2019 y se suscribió coincidente con los documentos de adjudicación el 118/10/2019; el acta de inicio se firmó el 07/11/2019.

Dado el objeto contractual, se revisó la propuesta presentada por el adjudicatario (hoy contratista) **O4IT COLOMBIA SAS**, a través de la plataforma SECOP II, y en particular, el Certificado de existencia y representación expedido por la Cámara de Comercio de Bogotá el 15/08/2019, en el que observa que se trata de una persona jurídica creada desde el 04/12/2008 con experiencia acreditada (RUP), entre otros, en temas de ciberseguridad o seguridad informática.

El contrato se encuentra en ejecución, con un plazo de 4 meses, que según se registra en el acta de inicio vencen el 06/03/2020.

Ahora bien, de la revisión legal específica se derivó el requerimiento al área auditada, efectuado mediante correo electrónico del 25/11/2019, en el que se solicitó la siguiente información:

> "*1. Constancia de entrega y aprobación de las hojas de vida del personal especializado según los "perfiles mencionados en el numeral 5 del anexo técnico".*
> *2. Plan de trabajo presentado para el desarrollo del contrato, junto con la constancia de entrega y aprobación por parte del supervisor del contrato*."

En consideración a la respuesta recibida mediante correo electrónico del mismo 25/11/2019, se realizó visita *in situ* el 02/12/2019, a efectos de precisar información y contenido en relación con:

- **Aprobación hojas de vida**: se indagó puntualmente sobre la fecha de presentación inicial de las hojas de vida (consultor senior y gerente de proyecto) y aprobación de la hoja de vida del gerente del proyecto, toda vez que el numeral 1, la cláusula 13.1 Obligaciones previas a la firma del acta de inicio, dispone: "*El contratista deberá presentar a los tres (3) días hábiles siguientes de firma del contrato, las hojas de vida del personal especializado a cargo del proyecto como requisito para la firma del acta de inicio, según los perfiles mencionados en el numeral 5 del anexo técnico y lo ofertado, a fin de que estas sean avaladas por el supervisor del contrato*", en el entendido de que el citado contrato se suscribió el 18/10/2019.

En la visita se revisaron correos electrónicos recibidos por el contratista de apoyo a la supervisión, en los que se evidenció la remisión de las hojas de vida oportunamente, el 23/11/2019 personal de la STRT puso a disposición una impresión del Plan de Trabajo presentado inicialmente por el contratista, de fecha 28/12/2018, cumpliendo en la presentación con el parámetro inicial.

En cuanto a la aprobación de la hoja de vida del gerente del proyecto, no se evidenció acta o documento de aprobación. Al respecto, según consta en el acta de visita, se puso a disposición la carpeta de ejecución del contrato en la que se observó que, teniendo en cuenta las observaciones formuladas a esta hoja de vida, el 29/10/2019, fue remitida por el enlace administrativo de la firma contratista la certificación con funciones que estaba pendiente para su aprobación. Manifestó el área auditada que: "*a pesar de la omisión documental (aprobación), esta actividad se realizó en la reunión del 07/11/2019, sin que quedara la anotación en el acta respectiva. Constancia de esto se dejará en el acta de la próxima reunión que se adelantará el próximo martes 3 de diciembre*".

Lo anterior evidencia nuevamente debilidades en el ejercicio de la supervisión del contrato, en contravención a lo dispuesto Manual de Interventoría y/o Supervisión de Contratos MG-GC-01, numeral "*6.1 Generalidades*", atendiendo la descripción y análisis efectuado para el contrato IDU-1520-2018.

- **Plan de trabajo y acuerdos de confidencialidad suscritos por el personal asignado al proyecto.** Se solicitó información particular sobre la oportunidad en su presentación, circunstancia que fue corroborada en la visita.

- **Aprobación de garantías (modificación por suscripción de acta e inicio).** Manifestó el área auditada que la DTGC aún no ha aprobado las garantías; por tanto, se recomienda realizar seguimiento al tema, ante la DTGC.

3.1 REQUISITOS CON INCUMPLIMIENTO

Nº	Criterio	Descripción
H1	**Procedimiento Generación de Copias de Seguridad, código PR-TI-11, versión 1.0**. *1.1.6.14 Guardar log* *"Esta actividad consiste en generar una copia de respaldo de los resultados arrojados por la herramienta de generación de copias, con el fin de conservar la evidencia de realización de las tareas ejecutadas. Dicho registro de eventos se conserva en el área de administración de copias según las disposiciones de conservación de registros vigentes."* *Ejecutantes* *Profesional Universitario* *1.2.1.11 Exportar logs* *"Una vez se culminan las tareas de generación de copias y de actualización de la disponibilidad de espacio, el funcionario encargado debe proceder a generar una copia de los archivos de registros automáticos de eventos de la herramienta de backup, como evidencia de la adecuada gestión del proceso y los conservará según las disposiciones vigentes de conservación de registros."* *Ejecutantes* *Profesional Especializado, Profesional Universitario.*	**Hallazgo Nº 1. Ausencia de copias de seguridad de los *logs* generados por la herramienta de generación de copias de seguridad.** No se evidenció la generación de copias de respaldo de los resultados arrojados por la herramienta de generación de copias, o de los archivos de registros automáticos de eventos de la herramienta de backup, situación que evidencia incumplimiento de los numerales "1.1.6.14 Guardar log" y "1.2.1.11 Exportar logs" del Procedimiento Generación de Copias de Seguridad, código PR-TI-11, versión 1.0 y que podría afectar trazabilidad de la información frente a las operaciones de copias efectuadas en el sistema.
H2	**Procedimiento PR-AC-07 Gestión de la Información Documentada** **1.5 POLÍTICA OPERACIONAL** […] *El primer responsable de garantizar que la documentación de un proceso es adecuada, pertinente y actual es el líder de proceso o el líder operativo. Por el ejercicio de autocontrol, deberán gestionar que el proceso cuente permanentemente con la documentación suficiente y necesaria para el logro de los objetivos del*	**Hallazgo Nº 2. Desactualización en el marco normativo de la documentación asociada a la estrategia de recuperación de desastres de TI.** Se evidenciaron situaciones que indican desactualización en el marco normativo de la documentación del proceso de Gestión de Tecnologías de Información y Comunicación, asociada a la estrategia de recuperación de desastres de TI, contraviniendo lo establecido en la política operacional del Procedimiento PR-AC-07 Gestión de la Información Documentada, situación que podría inducir a error o imprecisiones en decisiones o documentos que se adopten al interior del proceso y

Nº	Criterio	Descripción
	proceso y demás criterios definidos en su caracterización."	confusiones frente a responsabilidades y competencias en la ejecución de actividades en la entidad. Las situaciones específicas encontradas son las siguientes: a. Plan PL-TI-01 • Citan la "*Resolución Interna 6315 de 2016, "Por la cual se modifica y actualiza el Sistema de Coordinación Interna del IDU […]"*", la cual fue derogada por la Resolución IDU 2275 de 2018 (junio 1), a su vez, derogada por la Resolución IDU 5014 de 2018 (diciembre 20). • También, citan la Resolución 305 de 20 de octubre de 2008 "*Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre*" la cual fue modificada por la Resolución 004 de 2017 (noviembre 28) de la Comisión Distrital de Sistemas (CDS). Sin embargo, esta resolución no está incluida. • El Plan no relaciona la Resolución 1909 de 2019 (mayo 14), "*Por medio de la cual se define la política MIPG-SIG-IDU, se determinan las directrices y objetivos de los Subsistemas de Gestión, y se adopta la versión 4.0 del Manual de Procesos del IDU*". Esta resolución es importante toda vez que en sus artículos 12 y 13 adopta la Directriz del Subsistema de Gestión de Continuidad del Negocio (SGCN) y establece los respectivos objetivos. b. Procedimiento PR-TI-20 • Citan el Decreto 652 de 2011 de la Alcaldía Mayor de Bogotá "*Por medio del cual se adopta la Norma Técnica Distrital del Sistema Integrado de Gestión para las Entidades y Organismos Distritales*", el cual fue derogado por el artículo 14 del Decreto Distrital 591 de 2018. • Citan la "*Resolución 447 de 2012 del Instituto de Desarrollo Urbano: "Por la cual se reglamenta el Sistema Integrado de Gestión, se reorganiza su Sistema de Coordinación Interna y se crean los*

Nº	Criterio	Descripción
		equipos institucionales'", la cual fue derogada por la Resolución IDU 852 de 2019 (marzo 8), derogada a su vez por la Resolución IDU 1641 de 2019 (abril 26). • Citan la "*Resolución 6315 de 2016 del Instituto de Desarrollo Urbano: "Por la cual se modifica y actualiza el Sistema de Coordinación Interna del IDU, y se deroga la Resolución IDU 22477 de 2014 y sus modificaciones'"*", la cual fue derogada por la Resolución IDU 2275 de 2018 (junio 1), derogada a su vez por la Resolución IDU 5014 de 2018 (diciembre 20). • No está relacionada la Resolución 1909 de 2019, "*Por la cual se define la Política MIPG-SIG-IDU, se determinan las directrices y objetivos de los Subsistemas de Gestión, y se adopta la versión 4.0 del Manual de Procesos del IDU*". c. Instructivos IN-TI-03, IN-TI-23, IN-TI-24, IN-TI-25, IN-TI-26 e IN-TI-27 • Relacionan la *Norma Técnica NTC GP-1.000, Calidad en la gestión pública*, la cual no está vigente, tomando en cuenta que fue reemplazada por el modelo Integrado de Planeación y Gestión - MIPG (Decreto 1499/2017 y que fue adoptado en el Instituto con la Resolución 852 de 2019 (marzo 8), actualmente derogada por la Resolución IDU 1641 de 2019 (abril 26). • Citan la Resolución 305 de 20 de octubre de 2008 "*Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre*" la cual fue modificada por la Resolución 004 de 2017 (noviembre 28) de la Comisión Distrital de Sistemas (CDS). Sin embargo, esta resolución no está incluida. • Citan la "*Resolución 447 de 2012 del Instituto de Desarrollo Urbano: "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 fue derogada por la Resolución IDU 852 de 2019 (marzo 8),

Nº	Criterio	Descripción
		derogada a su vez por la Resolución IDU 1641 de 2019 (abril 26).
H3	**Manual de interventoría y/o supervisión de contratos - MG-GC-01 numeral 6.1 Generalidades**. *"La interventoría y la supervisión, junto con el equipo de apoyo a la supervisión de los contratos, de acuerdo con la naturaleza propia de las obligaciones/funciones a su cargo, deben exigir la calidad de los bienes, obras y servicios adquiridos en el marco de un contrato estatal, verificando que se cumplan todas las condiciones técnicas, económicas y legales pactadas. Para ello deberán garantizar que se cumplan las disposiciones legales y aquellas normativas internas del IDU, así mismo, deberán promover y verificar el cumplimiento de lo dispuesto en el respectivo contrato."* (Subrayado fuera de texto). **Contrato 1520-2018** **Cláusula 11, literal B, numeral 2. Obligaciones del Contratista.** "*Establecer un cronograma de trabajo donde se detalle las actividades de pre implementación, implementación y post-implementación donde se relacione los tiempos de ejecución y personal involucrado por Actividad, dentro de los cinco (5) días hábiles siguientes a la firma del Acta de Inicio*." **Contrato IDU-1522-2018** **Cláusula 11, literal B, numeral 1. Obligaciones del Contratista** "*Entregar un plan de trabajo, donde se establezcan las fechas de entrega, instalación y configuración de la solución ofertada. El cual debe ser aprobado por el supervisor del contrato, dentro de los dos (2) días hábiles siguientes a la firma del Acta de Inicio."* **Cláusula 11, literal B, numeral 5. Obligaciones del Contratista**	**Hallazgo No 3. Debilidades en el ejercicio de la Supervisión de contratos** Se evidenciaron debilidades en el ejercicio de la Supervisión de los contratos a cargo de la Subdirección Técnica de Recursos Tecnológicos, relacionadas particularmente con la documentación y seguimiento a las obligaciones contractuales en los contratos IDU-1520-2018, IDU-1522-2018 e IDU-1580-2019, contraviniendo lo dispuesto en el numeral "*6.1 Generalidades*" del Manual de Interventoría y/o Supervisión de Contratos, código MG-GC-01, situaciones que pueden generar demoras o deficiencias en la ejecución contractual. A continuación, se relacionan las situaciones evidenciadas: • Contrato 1520-2018 Cronograma: no se acreditó por parte del equipo auditado el cumplimiento de la condición temporal (fecha) de su presentación. • Contrato IDU 1522-2018 Plan de trabajo: se evidenció presentación extemporánea del Plan de trabajo. En cuanto a la Transferencia de conocimiento: Se acreditaron 7 y ½ horas de transferencia de conocimientos, las restantes, manifiesta el área se imputaron a acompañamiento presencial por parte del contratista; sin embargo, no se evidenció su cumplimiento; adicionalmente, la condición de 4 funcionarios receptores de la transferencia no se cumplió. • Contrato IDU-1580-2019. Aprobación hojas de vida: A pesar de presentar soportes que permiten inferir gestiones para la aprobación de la hoja de vida del Gerente del Proyecto, la aprobación formal no se gestionó documentalmente.

Nº	Criterio	Descripción
	"*Realizar una transferencia de conocimiento en las instalaciones del IDU, para cuatro (4) funcionarios con una intensidad horaria de mínimo cuarenta (40) horas sobre la configuración y administración de la plataforma implementada. Debe incluir material de estudio*". (Subrayado fuera de texto) **Contrato IDU-1580-2019.** **Cláusula 13.1, numeral 1. Obligaciones del Contratista** "*El contratista deberá presentar a los tres (3) días hábiles siguientes de firma del contrato, las hojas de vida del personal especializado a cargo del proyecto como requisito para la firma del acta de inicio, según los perfiles mencionados en el numeral 5 del anexo técnico y lo ofertado, a fin de que estas sean avaladas por el supervisor del contrato.*"	
H4	**Decreto 1081 de 2015, "*Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República*"** **Artículo 2.2.1.1.1.7.1. *Publicidad en el SECOP.*** *La Entidad Estatal está obligada a publicar en el Secop los Documentos del Proceso y los actos administrativos del Proceso de Contratación, dentro de los tres (3) días siguientes a su expedición.* […] **"*Artículo 2.1.1.2.1.8*** ***Publicación de la ejecución de contratos.*** *Para efectos del cumplimiento de la obligación contenida en el literal g) el del artículo 11 de la Ley 1712 de 2014, relativa a la información sobre la ejecución de contratos, el sujeto obligado debe publicar las aprobaciones, autorizaciones, requerimientos o informes del supervisor o del interventor, que prueben la ejecución del contrato*." **MANUAL DE INTERVENTORÍA Y/O SUPERVISIÓN DE CONTRATOS MG-**	**Hallazgo No. 4 Ausencia y/o extemporaneidad en la publicación en SECOP de información contractual** Se evidenció ausencia de publicación en el SECOP de las actas de liquidación de los contratos IDU-1520-2018 e IDU-1522-2018, que fueron remitidas a la Dirección Técnica de Gestión Contractual para el efecto, mediante memorandos 20195360112343 y 20195360112963 del 17/05/2019, respectivamente; como también, publicación extemporánea de todos los informes / constancias de ejecución del contrato IDU-PSP-1298-2019, lo cual contraviene lo dispuesto en los Artículos 2.1.1.2.1.7 y 2.1.1.2.1.8 del Decreto Único Reglamentario 1081 de 2015 y el sub numeral 12, del numeral 9.7.1 del Manual de Interventoría y/o Supervisión de Contratos, MG-GC-01, Versión 6.0, lo que conlleva a la afectación de los principios de transparencia, oportunidad y trazabilidad de la información. Es necesario precisar que en los memorandos 20125050215243, 20134350150453, 20174350188953, 20194350101733 y 20194350199723, se prevé la operatividad frente al tema.

Nº	Criterio	Descripción
	GC-01 Versión 6.0, numeral 9.7.1 Reglas de la Liquidación: […] "*12. Una vez suscrita el acta de liquidación, la dependencia a cargo del contrato deberá remitirla a la DTGC al día siguiente de su suscripción, para su publicación en los portales de contratación.*"	

4. RECOMENDACIONES/ OPORTUNIDADES DE MEJORA

De acuerdo con el desarrollo de la auditoría y los resultados obtenidos, a continuación, se relacionan las recomendaciones identificadas por el equipo auditor, conforme a la estructura y metodología implementadas, con el propósito de que el proceso de Gestión de las Tecnologías de la Información y las Comunicaciones, dentro de sus actividades de autocontrol, evalúe la pertinencia de incorporarlas en su gestión.

Adicionalmente, se precisa que, de acuerdo con lo establecido en las políticas de operación del procedimiento "Formulación, Monitoreo y Seguimiento a Planes de Mejoramiento", código PR-MC-01, V 7.0, "[...] *las recomendaciones realizadas en los Informes de auditoría, legales/obligatorios y seguimientos, realizados por la Oficina de Control Interno no obligan a dar tratamiento a través de Plan de mejoramiento y queda a potestad del responsable del proceso/dependencia, dar el tratamiento pertinente. No obstante, lo anterior, en caso que el líder de proceso/dependencia identifique la necesidad de registrar acciones, éstas deberán registrarse en el formato de Plan de mejoramiento adoptado en la entidad*".

A continuación, se presentan las recomendaciones identificadas por el equipo auditor:

1. Confirmar cuál es el procedimiento adecuado para adoptar la actualización del manual MG-TI-16 "Generación y Restauración de Copias de Seguridad", versión 3.0, toda vez que éste fue adoptado mediante Resolución 494 de 2017, con el fin de asegurar que no vayan a permanecer dos manuales vigentes. Esto es, verificar si es necesario efectuar la modificación o derogación de la resolución.

2. Tener en cuenta en la actualización del Manual de Generación y Restauración de Copias de Seguridad, código MG-TI-16, V 3.0 y los procedimientos relacionados con generación y restauración de copias de seguridad (PR-TI-11 y PR-TI-12), la revisión del Marco Normativo, de manera que se agregue la normatividad faltante y se elimine y/o reemplacen las normas derogadas o que no apliquen por las vigentes.

3. Considerar el ajuste de la política de planeación para la toma de copias de seguridad de acuerdo con la forma en la que efectivamente se realiza esta labor.

4. Establecer y documentar los criterios o parámetros para determinar la criticidad de los recursos o elementos a los cuáles se les toma copia de seguridad y, con base en ellos, identificar e incluir en las políticas de *backup* las relativas a la periodicidad y tipo de copiado y de tiempo de

retención en cinta y/o de permanencia en el sistema de almacenamiento, aplicables a cada recurso o tipo de recurso.

5. Revisar las actividades asignadas en el Manual de Generación y Restauración de Copias de Seguridad, código MG-TI-16, a los roles de Administrador del Centro de Cómputo y Operador de Copias de Seguridad, conciliarlas con el manual de funciones de los profesionales de planta o las obligaciones de los contratistas y diferenciar, en la práctica, quién ejecuta cada rol.

6. Evaluar la posibilidad de establecer una programación de restauración de copias de seguridad para asegurar que en cada año se incluyan, al menos una vez, una prueba de restauración de cada recurso.

7. Tener en cuenta en la actualización del Manual MG-TI-16 la eliminación de la referencia al formato FO-TI-24 “Bitácora de Control de Restauraciones de Copias de Seguridad” que fue derogado el 13/10/2017 y registrar, de ser el caso, la forma en la que se lleva el control de la restauración las copias de seguridad, identificando, en la medida de lo posible, si fueron a solicitud o las seleccionadas o definidas al azar por el administrador del centro de cómputo.

8. Verificar específicamente en qué archivo se debería llevar el control de las cintas que contienen las copias de seguridad y los datos que debe contener y, consecuentemente, hacer el ajuste en el Manual MG-TI-16 para que se ajuste a la realidad de la actividad.

9. Ajustar el alcance del Plan de Recuperación ante Desastres, código PL-TI-01, V 2, de manera que se indique, si es necesario, la existencia del equipo operativo mínimo durante la activación del DRP, o del listado de personas que lo conforman, pero retirando la referencia a que el listado está anexo al mismo. Igualmente, ajustar el encabezado del listado indicando que es el Anexo N° 2 del Plan o, en su defecto, eliminar el encabezado, de manera que no quede indicado que es un anexo.

10. Verificar la pertinencia de incluir el NIVEL OPERATIVO 2 en el formato FO-TI-26 “Árbol de Llamadas para DRP”, o efectuar la aclaración de por qué no se ha diligenciado, toda vez que pareciera estar diligenciado de manera incompleta. Así mismo, verificar quién asumiría las responsabilidades asignadas a este nivel.

11. Establecer y documentar directrices de revisión y actualización para el listado del “*EQUIPO OPERATIVO MÍNIMO DURANTE LA ACTIVACIÓN DEL DRP*” y del FO-TI-26 “Árbol de Llamadas para DRP”, de manera que se asegure que el personal registrado está vinculado al IDU y que sus datos son los correctos.

12. Precisar o especificar a qué se refieren los términos ‘formación’ y ‘divulgación’, relacionados en la quinta viñeta de la Política Operacional del documento del DRP. cada una de esas actividades.

13. Especificar la periodicidad o frecuencia real en la que se deberían efectuar pruebas al DRP.

14. Por lo cual se recomienda a la STRT coordinar con la SGGC y con la Oficina Asesora de Planeación para brindar capacitación u orientación a los participantes del DRP en los conceptos y documentos relacionados.

15. Coordinar con la SGGC y con la Oficina Asesora de Planeación para reforzar los conceptos y/o brindar capacitación u orientación a los participantes del DRP sobre los documentos y aspectos relacionados

16. Conciliar con la documentación del SGCN para determinar si es pertinente que la restauración de Valoricemos forme parte de la estrategia de DRP de servicios de TI

17. Efectuar el ajuste en la referencia al Plan de Continuidad de servicios de TI del alcance del Procedimiento Gestión de Continuidad de Servicios de TI, PR-TI-20, dado que fue reemplazado por el Plan de Recuperación ante Desastres, PL-TI-01.

18. Identificar y/o establecer criterios que permitan determinar cuando algún incidente o evento pueda clasificarse como situación de emergencia que dé lugar a la recuperación de los servicios de TI afectados o al inicio del DRP.

19. Verificar, cada que se vaya a efectuar el monitoreo y/o actualización de los riesgos, la utilización de formatos vigentes, con el fin de que la calificación de probabilidad, impacto, riesgo inherente y riesgo residual esté acorde con las directrices respectivas.

20. Evaluar la construcción y pertinencia de los controles planteados en las matrices de riesgos del proceso de Gestión de Tecnologías de la Información y la Comunicación, teniendo en cuenta que éstos deben tener un propósito que indique para qué se realizan y deben llevar a prevenir las causas que generan el riesgo o a detectar su materialización. En este sentido, se sugiere identificar en la matriz de riesgos del proceso, para cada causa, cuáles son sus controles, tomando en cuenta que para cada una debe existir, mínimo, un control.

21. Revisar cada uno de los controles registrados en la matriz de riesgos, identificando específicamente los responsables, periodicidad de ejecución, cómo se hace, dónde queda evidenciada su utilización o aplicación y las indicaciones de qué pasa cuándo se encuentran desviaciones u observaciones una vez es ejecutado.

22. Incorporar al expediente ORFEO de los contratos a su cargo todos los documentos, comunicaciones y soportes de la contratación y que soporten la ejecución contractual.

23. Realizar seguimiento a la aprobación de garantías (modificadas por suscripción de acta de inicio), por parte de la DTGC en desarrollo del contrato IDU-1580-2019.

5. CONCLUSIONES

De acuerdo con las actividades verificadas y los criterios establecidos para la auditoría, en términos generales, se evidenció que el proceso cuenta con instrumentos para la planeación, seguimiento y control de sus operaciones; sin embargo, se evidenciaron requisitos con incumplimiento asociados con:

- Ausencia de copias de seguridad de los *logs* generados por la herramienta de generación de copias de seguridad.

- Desactualización en el marco normativo de la documentación asociada a la estrategia de recuperación de desastres de TI.
- Debilidades en el ejercicio de la Supervisión de contratos.
- Ausencia y/o extemporaneidad en la publicación en SECOP de información contractual.

A continuación, se presenta el resumen de los resultados:

Total N°. de Hallazgos	Total N°. de Recomendaciones
4	23

6. ANEXOS

Anexo. Análisis Matriz Riesgos de Corrupción.

7. EQUIPO AUDITOR

ORIGINAL FIRMADO
ISMAEL MARTÍNEZ GUERRERO
Jefe de Control Interno

ORIGINAL FIRMADO
ADRIANA MABEL NIÑO ACOSTA
Auditor líder

ORIGINAL FIRMADO
ERIKA MARÍA STIPANOVIC VENEGAS
Auditor acompañante