ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2023-26563
Fecha: 24/07/2023 06:07:46 PM - Anexos:
Destino: 100-DESPACHO

MEMORANDO

Para: OSCAR ANTONIO GOMEZ HEREDIA
DESPACHO SECRETARIO DE SEGURIDAD

De: OFICINA DE CONTROL INTERNO

Asunto: INFORME FINAL DE AUDITORÍA AL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.

Cordial saludo, Doctor Gómez Heredia:

La Oficina de Control Interno, en su rol de evaluación y seguimiento y dando cumplimiento al Plan Anual de Auditoria de la vigencia 2023, aprobado en el Comité Institucional de Coordinación de Control Interno, se permite comunicar el Informe Final de Auditoría al **Proceso de Gestión de Tecnologías de la Información**.

Cabe informar que el presente informe fue socializado con la Dirección de Tecnologías y Sistemas de Información en reunión de cierre de auditoría tal como lo define el procedimiento de "Auditoría Interna". En dicha sesión el proceso auditado presentó comentarios los cuales la Oficina de Control Interno aceptó y procedió a ajustar para las observaciones No 13, 15, 18, 23 y 35; nos permitimos aclarar que las mencionadas observaciones se modificaron en aspectos puntuales, no obstante, las mismas se mantienen en el informe debido a que la causas de estas permanecen; las restantes observaciones y oportunidades de mejora comunicadas en el informe preliminares fueron aceptadas por la DTSI.

A partir de los resultados de la auditoría realizada, se deberá formular los planes de mejoramiento a que haya lugar y por solicitud del proceso auditado, es necesario que las siguientes observaciones se aborden de manera articulada y así generar mejoras transversales a la Entidad:

OBSERVACIÓN	DEPENDENCIA
Observación N°12	• Oficina Centro de Comando, Control y Comunicaciones-C4
Observación N°20 y 21	• Oficina de Análisis de Información y Estudios Estratégicos
Observación N° 28,29 y 30	• Dirección de Recursos Físicos y Gestión Documental

El plan de mejoramiento se deberá cargar en el aplicativo ITS-Portal MIPG, razón por la cual se remite copia del presente informe a la Oficina Asesora de Planeación, esto con el propósito de que se brinde el apoyo y/o asesoría metodológica para la identificación de la causa raíz, formulación y registro del plan de mejoramiento interno en el aplicativo en mención de acuerdo con lo establecido en el procedimiento "Plan de Mejoramiento Interno PD-SM-4" Versión 5.

Av. Calle 26 # 57- 83
Torre 7 Tel: 3779595
Código Postal: 111321
www.scj.gov.co

ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2023-26563
Fecha: 24/07/2023 06:07:46 PM - Anexos:
Destino: 100-DESPACHO

El tiempo máximo para la formulación y registro del plan de mejoramiento interno por parte del Líder del Proceso auditado será de ocho (8) días hábiles, contados a partir de la comunicación y/o notificación que generará el aplicativo mencionado.

Finalmente, la Oficina de Control Interno realizará la verificación de las acciones propuestas en términos de eficiencia y eficacia, no obstante, es de anotar que, como primera línea de defensa en el marco del Modelo Integrado de Planeación y Gestión, le compete al proceso de Gestión de Tecnologías de la Información hacer seguimiento al cumplimiento de dicho plan.

Cordialmente,

KAROL ANDREA PARRAGA HACHE
JEFA OFICINA DE CONTROL INTERNO

c.c.e.: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
RAFAEL MAURICIO SOPO-DIRECCION DE RECURSOS FISICOS Y GESTION DOCUMENTAL
JUAN DAVID GARCIA RUEDA-OFICINA ASESORA DE PLANEACION
SAYRA GUINETTE ALDANA HERNANDEZ-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
ADA LUZ SANDOVAL HERAZO-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
Anexo: 1
Anexos Digitales: 1

Elaboró: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO
Revisó: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO |
Aprobó: KAROL ANDREA PARRAGA HACHE-OFICINA DE CONTROL INTERNO

Av. Calle 26 # 57- 83
Torre 7 Tel: 3779595
Código Postal: 111321
www.scj.gov.co

Informe Final de Auditoría al Proceso Gestión de Tecnologías de la Información

2023

Oficina de Control Interno

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

TABLA DE CONTENIDO

1. GENERALIDADES DE LA AUDITORÍA

OBJETIVO	Evaluar y verificar la aplicación de los procedimientos y la gestión de los riesgos asociados al proceso de Gestión de Tecnologías de Información documentados en el Sistema Integrado de Gestión y demás criterios asociados.
OBJETIVOS ESPECÍFICOS	- Validar el grado de cumplimiento y alineación de los procedimientos seleccionados en muestra. - Evaluar la efectividad de los controles establecidos a los riesgos asociados al proceso de Gestión de Tecnologías de Información. - Revisar el cumplimiento, alineación y actualización del PETIC de la Entidad, debido a su importancia e impacto sobre todo el proceso de Gestión de Tecnologías de Información. - Validar la política de seguridad de la información de la Entidad. - Verificar el cumplimiento de las metas del proyecto "7777 Fortalecimiento de la gestión de las Tecnologías de la Información en la Secretaría de Seguridad, Convivencia y Justicia en el marco de las políticas de gobierno y seguridad digital en Bogotá" con corte al primer trimestre de 2023.
ALCANCE	El alcance de la auditoría consiste en la evaluación al proceso Gestión de Tecnologías de Información, a partir de los procedimientos y aplicación, así como, la gestión de los riesgos asociados al proceso y la ejecución de los recursos asignados a través del proyecto de inversión a su cargo para el periodo comprendido entre el 01 de enero de 2022 hasta el 31 de marzo de 2023. En el desarrollo de la auditoría puede realizarse solicitud de documentos o aspectos del procedimiento con fecha anterior o posterior al periodo planteado, según la necesidad que surja en el desarrollo de la auditoría.
METODOLOGÍA	♦ Solicitudes de información ♦ Reuniones o mesas de trabajo con el personal relacionado con los procedimientos. ♦ Verificaciones y confirmaciones documentales. ♦ Entrevistas y/o Indagaciones ♦ Aplicación de listas de verificación. ♦ Validaciones en página web e intranet de la Entidad, así como también se requerirá acceso a repositorios de información para los casos que aplique. ♦ Análisis y cotejo de información.
INFORME EJECUTIVO	En el presente informe, se reflejan los resultados obtenidos en el ejercicio de la auditoría al proceso de Gestión de Tecnologías de Información de la Secretaría de Seguridad Convivencia y Justicia, el cual es liderado por la Dirección de Tecnologías y Sistemas de la Información en adelante se denominará DTSI; la auditoría se llevó a cabo en el trimestre comprendido entre abril a junio de la presente vigencia. El objetivo principal de esta auditoría fue evaluar la manera de cómo están funcionando actualmente los procedimientos oficializados en el sistema integrado de gestión adscritos al proceso, pasando por la evaluación de lineamientos y políticas como la de seguridad y privacidad de la información, el plan estratégico de sistemas de la información PETI, los riesgos y con sus respectivos controles, las metas, entre otros aspectos de carácter relevante de cara al soporte que el ámbito tecnológico da a la misionalidad de la Secretaría. Lo anterior, a través de un análisis independiente y objetivo, donde se identificaron fortalezas y temas de

	mejora las cuales al ser atendidos permiten que se fortalezca el ambiente de control y que se cumpla la normativa existente a nivel Distrital y Nacional en materia TIC. Temas claves validados: ✓ Riesgos asociados al proceso y riesgos de corrupción: Se realizó evaluación de nueve (9) riesgos de gestión y dos (2) riesgos de corrupción, donde el principal aspecto se asoció a la revisión del diseño y solidez tanto en los eventos de riesgo como en los controles establecidos, generando observaciones u oportunidades de mejora en términos de estructura, redacción, clasificación y evidencia documental. Se insta al proceso a revisar y ajustar los riegos con el fin de dar cumplimiento a la Política de Administración de Riesgos establecida por la entidad. ✓ Metas asociadas a los proyectos: El proyecto de inversión 7777, con corte a 31/03/2023, realizó un avance en la ejecución física entre el 15% y 24%, así como un compromiso entre el 10% y 100% y un giro presupuestal entre el 2% y 6%, teniendo en cuenta que el proyecto se encuentra en ejecución se recomienda realizar seguimientos periódicos a la ejecución física, ejecución de la vigencia, las reservas y pasivos exigibles del proyecto con el objetivo de tomar las medidas necesarias para su pago o depuración asegurando una adecuada gestión financiera para su utilización efectiva. ✓ Plan estratégico de tecnologías de la información PETI: Este documento funciona como carta de navegación y principalmente describe la misión y visión qué se tiene para el ámbito tecnológico de la Secretaría. El documento está planteado para el cuatrienio y de manera general se informa que se encuentra alineado y se ha cumplido con el propósito allí propuesto. El principal aspecto por mencionar es la actualización y alineación del PETI frente a los documentos guía emitidos por el MINTIC. ✓ Procedimientos asociados: El proceso de Gestión de Tecnologías de la Información requiere una actualización general a sus procedimientos, permitiendo dar cuenta y estar alienados con las actividades que se desarrollan y ejecutan en el día a día, principalmente al interior de la Dirección de Tecnologías y Sistemas de la Información; adicionalmente se requiere la revisión y adición de puntos de control que garanticen el cumplimiento y flujo de estos procedimientos. Por otra parte, se requiere fortalecer la generación de soportes y evidencias contemplados en cada una de las actividades, situación que debe ser revisada en la actualización que se está llevando a cabo por el proceso. ✓ Seguridad de la información: Se observó conciencia sobre la seguridad de la información en la Entidad, esto por medio de la implementación de medidas y lineamientos orientados hacia la protección de los datos y la información de la Entidad apoyado en una infraestructura de seguridad informática la cual ha sido adquirida a través de las vigencias. Una vez mencionado lo anterior, en el ejercicio auditor se identificaron situaciones sobre la generación de documentación, administración y gestión de usuarios de los sistemas de información, fortalecimiento en la aplicación de los controles de acceso físico, gestión de vulnerabilidades y plan de continuidad del negocio en materia de tecnología. ✓ Uso y apropiación: El fortalecimiento del tema de uso y apropiación del ámbito tecnológico es crucial para garantizar que los recursos tecnológicos sean utilizados de manera efectiva, beneficiosa y sincrónica para la Entidad, por tanto, es un tema que se resalta para que se generen iniciativas y actividades por parte de la DTSI y así lograr que los usuarios se apropien y apliquen las metodologías y lineamientos que se establezcan.

Tabla N°01. Elaboración Propia OCI – Generalidades de la Auditoría.

2. RESULTADOS DEL EJERCICIO DE AUDITORÍA

3.1 RIESGOS DEL PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Se verificaron un total de nueve (9) riesgos activos en la Matriz de Riesgos por Proceso V29 publicada en la página web de la Entidad[1] el 29 de marzo de 2023, así como los cambios realizados por el proceso (1LD) con asesoría de la Oficina Asesora de Planeación (2LD)[2] a corte de 30 de marzo de 2023 en el marco de la Política de Administración del Riesgo V7 publicada en el portal MIPG. A continuación, se muestran los riesgos por tipo de impacto y tipología:

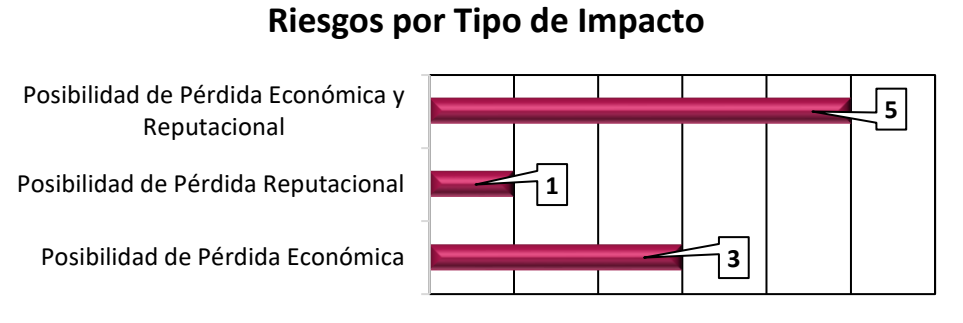


Gráfico N°01. Elaboración propia: Fuente: Matriz de riesgos por proceso V29

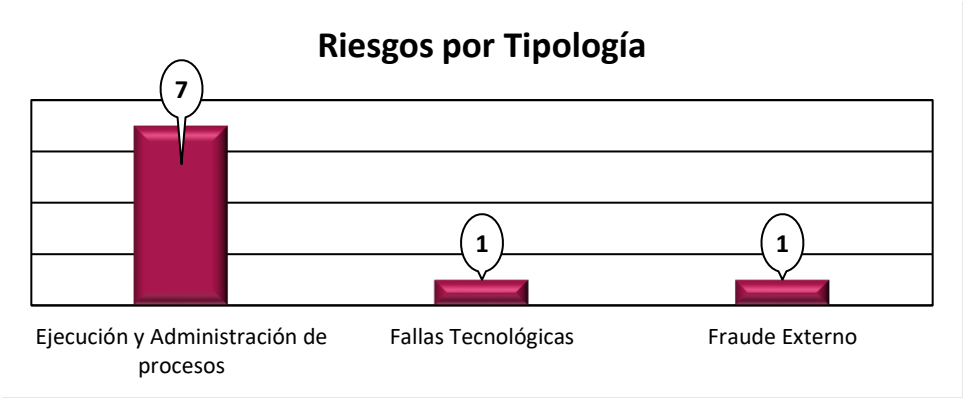


Gráfico N°02. Elaboración propia: Fuente: Matriz de riesgos por proceso V29

Se procedió a validar la solidez de los riesgos establecidos por el proceso de acuerdo con la metodología señalada en la Política de Administración del Riesgo V7 de la Entidad y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5 del 2020 emitida por el Departamento Administrativo de la Función Pública. A continuación, se presentan los resultados:

CRITERIO/ RIESGO	R1GT	R2GT	R3GT	R4GT	R5GT	R6GT	R7GT	R8GT	R9GT
Redacción del riesgo (impacto + causa inmediata + causa raíz)	Redacción Adecuada	Redacción Adecuada	Redacción Adecuada	Redacción Adecuada	Redacción similar al R6	Redacción similar al R5	Redacción Similar al R8	Redacción similar al R7	Redacción Adecuada

[1] Matriz de Riesgos por Proceso V29 https://scj.gov.co/sites/default/files/planeacion/Matriz%20General%20de%20Riesgos%20por%20Proceso%20F-DS-575%20V29%20-%20General.xlsx

2 Ajuste en la redacción del Control 2 y 3 del R5GT y ajuste en la redacción del Control 1 Riesgo R9GT

CRITERIO/ RIESGO	R1GT	R2GT	R3GT	R4GT	R5GT	R6GT	R7GT	R8GT	R9GT
Adecuada clasificación del Riesgo	Clasificación coherente con la descripción del riesgo	Clasificación coherente con la descripción del riesgo	Clasificación coherente con la descripción del riesgo	Clasificación coherente con la descripción del riesgo	Clasificación coherente con la descripción del riesgo	Clasificación coherente con la descripción del riesgo	Clasificación coherente con la descripción del riesgo	Clasificación incoherente con la descripción del riesgo	Clasificación coherente con la descripción del riesgo
Solidez del Riesgo (Severidad después de aplicar el control)	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Moderado	Moderado	Moderado
¿Posee un plan de contingencia asociado?	N/A	N/A	N/A	SI	N/A	N/A	SI	SI	SI

Tabla 02. Elaboración propia: Fuente: Política administración del riesgo

OBSERVACIÓN N° 1 Debilidades en el diseño, estructura y clasificación de los riesgos N°5, N°6, N°7 Y N°8 en términos de redacción, identificación de causa - consecuencia y análisis del contexto estratégico del proceso:

De acuerdo con la revisión del diseño y estructura de los riesgos asociados al proceso, se identificaron riesgos similares en su redacción, al verificar que las causas inmediatas de los riesgos N°5 y N°6 están orientadas a "*insatisfactoria calificación por parte de las partes interesadas en la prestación de servicios del proceso y/o incumplimiento normativo*". De igual forma los riesgos N°7 y N°8 contienen como causa raíz la "*insuficiente divulgación y socialización de la política de seguridad digital…*"**.**

Paralelamente, se identificaron debilidades en la clasificación del riesgo N°8 titulado "fraude externo" respecto al análisis e identificación del contexto estratégico del proceso al catalogarlo como *"pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la Entidad)"*, ya que no tiene relación con el riesgo de un posible incumplimiento del plan de seguridad de la información que se implementa cada año en la Entidad.

Lo anterior, denota un incumplimiento con lo establecido en la Política de Administración del Riesgo de la Entidad V7 al no aplicar correctamente la metodología referente al análisis de los eventos de riesgos de proceso, análisis e identificación del contexto estratégico del proceso y las causas que determinan el riesgo, lo que puede afectar de manera negativa el logro de los objetivos del proceso.

RECOMENDACIÓN N° 1 : Revisar y ajustar la clasificación del riesgo "*Posibilidad de pérdida Reputacional y Económica por Incumplimiento normativo, rezago en la trasformación digital de la Entidad, o posible incumplimiento del plan de seguridad de la información que se implementa cada año en la Entidad (Baja implementación de los controles del Anexo A de la norma ISO 27001), o perdida de información o aumento en la probabilidad de ataques cibernéticos debido a la insuficiente divulgación y socialización de la Política de Seguridad Digital por parte de los demás procesos, o indisponibilidad del talento humano al interior de los procesos para implementar la política, o indisponibilidad o no asignación suficiente de recursos presupuestales para implementar la política, o falta de seguimiento a la implementación de la política*" de acuerdo a las definiciones que provee la Guía para la administración del riesgo y el diseño de controles en Entidades Públicas v5 del 2020 del Departamento de la Función Pública.

Complementando la verificación, se evaluó la estructura para la descripción de los controles asociados a los riesgos del proceso así:

¿Tiene un responsable?	¿Cuenta con una periodicidad?	¿Tiene definido un soporte?
		
100% de los controles cuentan con un responsable para ejecutar la acción.	93,7% de los controles delimitan la periodicidad de ejecución del control.	100% de los controles cuentan con la evidencia que respalda su ejecución.

Tabla N°03. Elaboración propia: Fuente: Matriz de riesgos por proceso V29 publicada en la página web de la Entidad

OBSERVACIÓN N° 2: Debilidades en la estructura del control N°1 asociado al riesgo N° 9.:
Esta observación se expresa toda vez que no se especifica la periodicidad de ejecución del control, siendo este uno de los criterios establecidos en la Política de Administración del Riesgo de la Entidad V7 en el numeral 10.7.1, lo que puede derivar en la materialización del riesgo.

RECOMENDACIÓN N° 2: Revisar y ajustar la descripción del control "*El (la) Director(a) de Tecnologías y Sistemas de la Información convoca y lidera la ejecución de las sesiones que se establezca de manera conjunta para estructurar y validar que el diseño, desarrollo y puesta operación de la solución tecnológica estén acorde las necesidades identificadas con los líderes de procesos. En el evento que no contar con la asistencia alguno de los líderes de procesos, se generaran las comunicaciones a que haya lugar para socializar la información. Como evidencia de la ejecución del control se contará con comunicación de invitación a la sesión de validación, acta de dicha sesión y de las que se lleven a cabo. El cargue de las evidencias se hará trimestralmente*", en lo referente a incluir la periodicidad de ejecución de las sesiones. Esto se debe realizar por parte de la DTSI con la asesoría de la OAP.

Adicionalmente, se verificó que los controles diseñados estuviesen orientados a prevenir, corregir y/o detectar la causas raíz, con el fin de lograr una adecuada mitigación de los riesgos asociados, obteniendo los siguientes resultados:

Tipo de control	Descripción	Total de Controles vigentes del proceso
Preventivo	Control accionado en la entrada del proceso	16
Correctivo	Control relacionado accionado en la salida del proceso	0
Detectivo	Control accionado durante la ejecución del proceso	0

Tabla N°04. Elaboración Propia OCI – Fuente: Matriz de Riesgos por Proceso V29

OPORTUNIDAD DE MEJORA N° 1: Debilidades en la aplicación de la metodología de riesgos asociados al proceso:
El proceso de Gestión de Tecnologías de la Información estableció para el manejo de sus riesgos un total de dieciséis (16) controles bajo la tipología de preventivos; es decir, asociados a atacar la probabilidad de ocurrencia del riesgo[3], sin embargo, no se identificaron controles correctivos o detectivos que ataquen el impacto frente a la materialización del riesgo.

[3] Guía para la administración del riesgo y el diseño de controles en Entidades públicas, versión 5 de diciembre de 2020.

RECOMENDACIÓN N° 3: Realizar un análisis e identificación de controles por parte de la DTSI que permitan adelantar acciones de verificación y seguimiento no solo durante las actividades de ejecución del proceso sino también en los productos y/o resultados que genere, con la finalidad de atacar no solo la probabilidad de ocurrencia sino también el impacto frente a la materialización del riesgo.

3.2 RIESGOS DE CORRUPCIÓN DEL PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Se procedió a realizar la evaluación de efectividad de los riesgos identificados, analizados, valorados por la primera línea de defensa, así como la ejecución de sus actividades de control, lo anterior, de acuerdo con la Matriz de Riesgos de Corrupción V21 de la Entidad, publicada en la página web[4] y en el marco de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V4 de 2018 emitida por el Departamento Administrativo de la Función Pública así:

N° Riesgos Corrupción	N° Control	¿Tiene un responsable definido?	¿Tiene una periodicidad definida?	¿Se indica cual es el propósito del Control?	¿Se establece como se realiza la actividad de control?	¿Tiene manejo de la desviación?	¿El control tiene evidencia?	Resultado del diseño del control
R1	Control 1	Asignado	Oportuna	Previene	Confiable	Se investigan y resuelven oportunamente	Incompleta	MODERADO
	Control 2	Asignado	Oportuna	Previene	Confiable	Se investigan y resuelven oportunamente	Completa	FUERTE
R2	Control 1	Asignado	Oportuna	Detecta	Confiable	Se investigan y resuelven oportunamente	Completa	FUERTE
	Control 2	Asignado	Oportuna	No tiene propósito	Confiable	Se investigan y resuelven oportunamente	Completa	MODERADO

Tabla N°05. Elaboración propia. Fuente: Matriz de Riesgos de Corrupción v21

OPORTUNIDAD DE MEJORA N° 2: Debilidad en el diseño de los controles en términos de identificación del propósito y evidencia documental:

La evidencia establecida para la ejecución de la actividad de control N°1 asociado al riesgo N°2 está orientado a la verificación del cumplimiento del plan de uso y apropiación, pero el soporte de ejecución del control es "*listas de asistencia, cronograma y presentaciones del proceso de divulgación*" únicamente responde a una parte de las actividades que se realizan en el marco del plan; así las cosas, estas dos variables (propósito y evidencia) del diseño del control deben estar relacionadas y la evidencia debe dar cuenta del 100% de acciones que se realizan para la adecuada mitigación del riesgo.

4matriz general de riesgos de corrupcion sdscj v21 – 2023
https://scj.gov.co/sites/default/files/planeacion/Matriz%20General%20de%20Riesgos%20de%20Corrupcion%20SDSCJ%20V21%20%282%29.xlsx

Así mismo, la redacción del control N°2 asociado al riesgo N°2 no contiene de manera clara el propósito que indique para qué se realiza la actividad de control "*reporte de monitoreo cuatrimestral mitiga la causa del riesgo*".

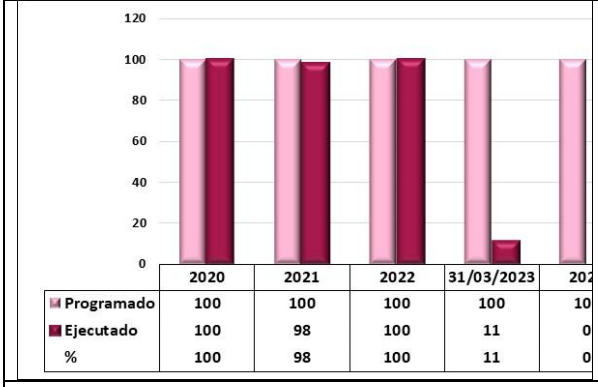
RECOMENDACIÓN N° 4: Revisar y ajustar por parte de la DTSI el diseño de los controles de acuerdo con los lineamientos establecidos por la Política de Administración del riesgo de la Entidad V7.

3.3 PROYECTO DE INVERSIÓN 7777 - FORTALECIMIENTO DE LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LA SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA EN EL MARCO DE LAS POLÍTICAS DE GOBIERNO Y SEGURIDAD DIGITAL EN BOGOTÁ.

De acuerdo con la clasificación de la estructura del Plan de Desarrollo registrada en la ficha EBI del Proyecto de Inversión 7777, este se encuentra relacionado con el propósito 05 ***"Construir Bogotá Región con gobierno abierto, transparente y ciudadanía consciente"*** y el programa general 54 "*Transformación digital y gestión de TIC para un territorio inteligente".* Por otra parte, el proyecto de inversión cuenta con 8 metas, de acuerdo con el alcance de la auditoría se realizó verificación de lo registrado en la herramienta SEGPLAN con corte a 31 de marzo de 2023 encontrando:

- **Meta 1 Mantener al 100 por ciento la disponibilidad de los componentes de infraestructura y servicios tecnológicos mediante la administración, operación, mantenimiento y soporte de estos.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	100% Meta Constante	$ 7.449	$ 27.579



	2020	2021	2022	31/03/2023	202
Programado	100	100	100	100	10
Ejecutado	100	98	100	11	0
%	100	98	100	11	0

	2020	2021	2022	31/03/2023	2024
Programado	$ 1.847	$ 7.337	$ 6.926	$ 7.449	$ 4.019
Ejecutado	$ 1.832	$ 6.459	$ 6.791	$ 770	$ 0
%	99,17	88,02	98,06	10,34	0

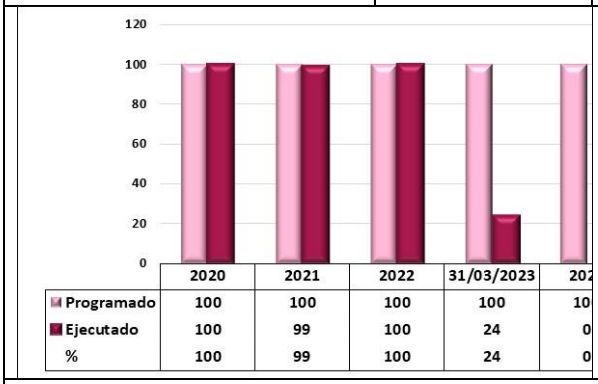
Análisis OCI: Teniendo en cuenta los datos registrados en SEGPLAN con corte a 31/03/2023, se pudo determinar una ejecución de la magnitud del 11% soportado en el mantenimiento de la infraestructura tecnológica para la operación de la SDSCJ, por otra parte, avanzaron en la ficha técnica de los procesos relacionados con la meta.

En lo referente a la ejecución presupuestal se observó un total comprometido del 10,34% y un giro acumulado de $48.681.060 lo cual corresponde al 6% de lo comprometido con corte a 31/03/2023.

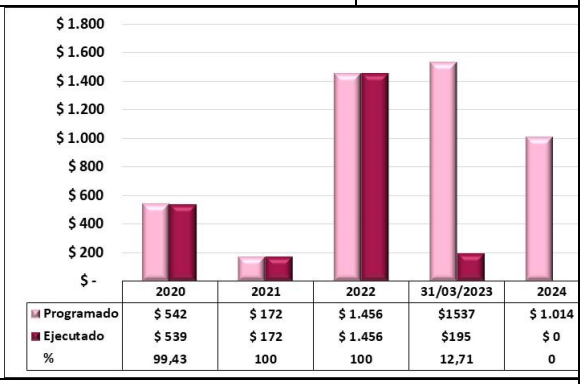
*Tabla N°06. Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023. Nota: *Cifras Millones de pesos.*

- **Meta 2 Planear y ejecutar al 100 por ciento la estrategia para la actualización de los servicios tecnológicos existentes e implementación de nuevos, que optimicen la productividad de la Entidad en el marco de la gestión por procesos.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	100% Meta Constante	$ 1.537	$ 4.721



	2020	2021	2022	31/03/2023	202
Programado	100	100	100	100	10
Ejecutado	100	99	100	24	0
%	100	99	100	24	0



	2020	2021	2022	31/03/2023	2024
Programado	$ 542	$ 172	$ 1.456	$1537	$ 1.014
Ejecutado	$ 539	$ 172	$ 1.456	$195	$ 0
%	99,43	100	100	12,71	0

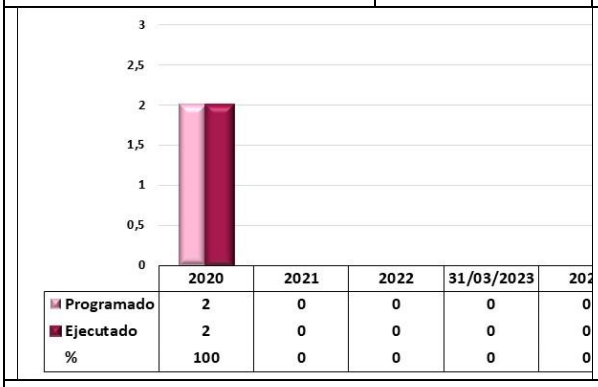
Análisis OCI: Teniendo en cuenta los datos registrados en SEGPLAN con corte a 31/03/2023, se pudo determinar una ejecución de la magnitud del 24% soportado en la actualización y avance del plan para actualización de servicios tecnológicos de la SDSCJ. El avance corresponde al diseño de la propuesta de servicios de redes de comunicación, servicio de telefonía IP, servicio de impresión, fotocopiado y escaneo, mesa de servicios y servicio de disposición y soporte de bienes tecnológicos.

En lo referente a la ejecución presupuestal se observó un total comprometido del 12,71% y un giro acumulado de $3.100.000 lo cual corresponde al 2% de lo comprometido con corte a 31/03/2023.

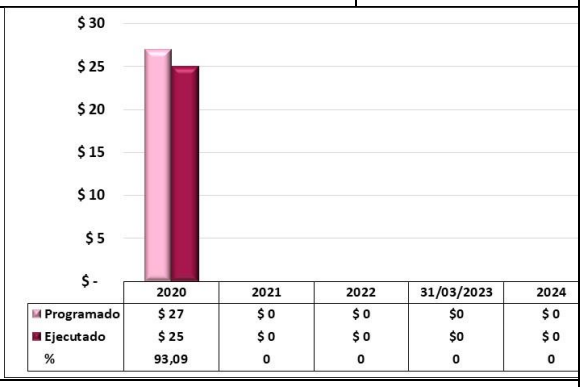
*Tabla N°07. Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023. Nota: *Cifras Millones de pesos.*

- **Meta 3 Realizar 2 campañas de sensibilización a servidores públicos y contratistas en temas de tic para fortalecer el uso y apropiación de los servicios tecnológicos.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	Dos Campañas Suma	$ 0	$ 27



	2020	2021	2022	31/03/2023	202
Programado	2	0	0	0	0
Ejecutado	2	0	0	0	0
%	100	0	0	0	0



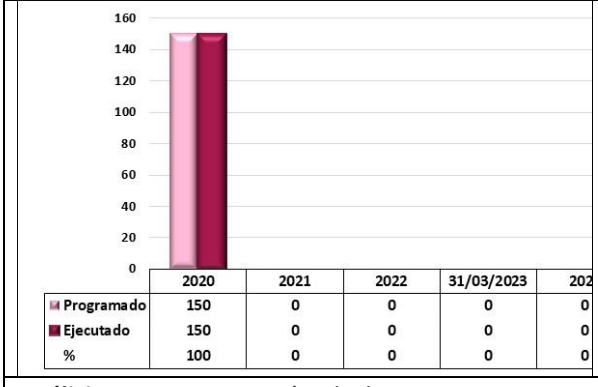
	2020	2021	2022	31/03/2023	2024
Programado	$ 27	$ 0	$ 0	$0	$ 0
Ejecutado	$ 25	$ 0	$ 0	$0	$ 0
%	93,09	0	0	0	0

Análisis OCI: La ejecución de la meta se programó para dar cumplimiento en la vigencia 2020, en concordancia con lo anterior, no se observó recursos programados para los años 2021, 2022, 2023 y 2024. La meta se encuentra en estado finalizada.

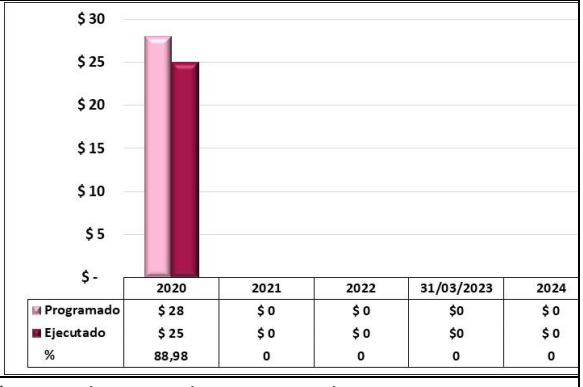
*Tabla N°08. Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023. Nota: *Cifras Millones de pesos.*

- **Meta 4 Capacitar a 150 servidores públicos y contratistas en temas de tic para fortalecer el uso y apropiación de los servicios tecnológicos.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	150 Servidores Públicos - Suma	$ 0	$ 28



	2020	2021	2022	31/03/2023	202
Programado	150	0	0	0	0
Ejecutado	150	0	0	0	0
%	100	0	0	0	0



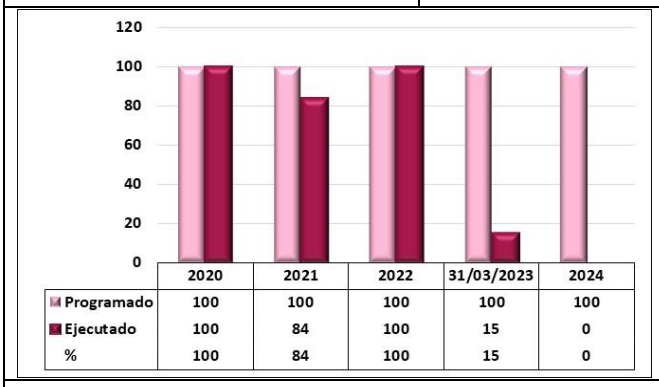
	2020	2021	2022	31/03/2023	2024
Programado	$ 28	$ 0	$ 0	$0	$ 0
Ejecutado	$ 25	$ 0	$ 0	$0	$ 0
%	88,98	0	0	0	0

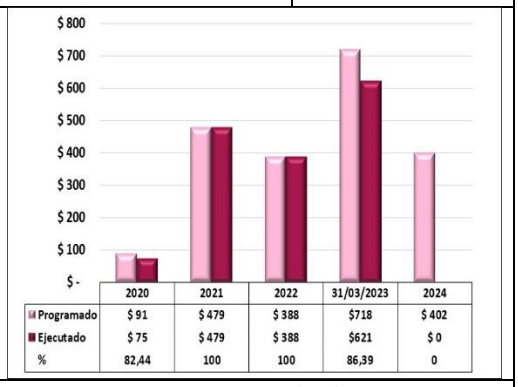
Análisis OCI: La ejecución de la meta se programó para dar cumplimiento en la vigencia 2020, en concordancia con lo anterior, no se observó programación de recursos para los años 2021, 2022, 2023 y 2024. La meta se encuentra en estado finalizada.

*Tabla N°09. Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023. Nota: *Cifras Millones de pesos.*

- **Meta 5 Planear y ejecutar al 100 por ciento la estrategia para la actualización de los servicios ciudadanos digitales existentes e implementación de nuevos, acordes a la normatividad vigente y las necesidades identificadas de los ciudadanos.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	100% Meta Constante	$ 718	$ 2.077





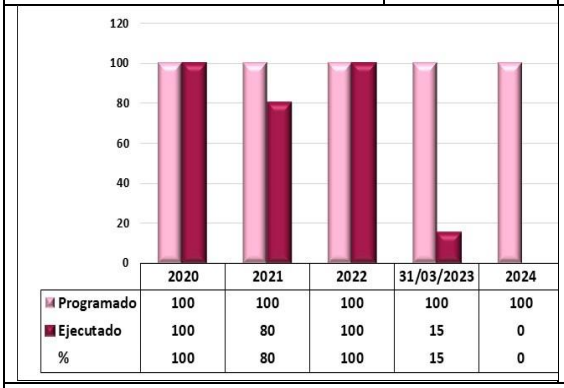
Análisis OCI: Teniendo en cuenta los datos registrados en SEGPLAN con corte a 31/03/2023, se pudo determinar una ejecución de la magnitud del 15% soportado en la ejecución de actividades como evaluación de los 15 servicios ciudadanos digitales, se determinó los servicios con menos uso y mesas de trabajo para definir la estrategia.

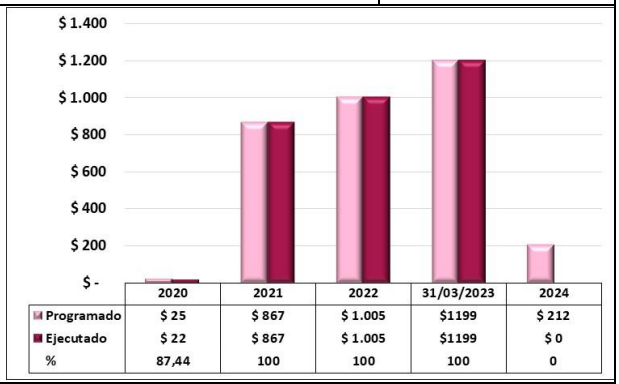
En lo referente a la ejecución presupuestal se observó un total comprometido del 86,39% y un giro acumulado de $11.775.000 lo cual corresponde al 2% de lo comprometido con corte a 31/03/2023.

*Tabla N°10. Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023. Nota: *Cifras Millones de pesos.*

- **Meta 6 Planear y ejecutar al 100 por ciento la estrategia para la actualización de los documentos asociados con el dominio de gobierno de ti, de acuerdo con los lineamientos distritales, nacionales y las mejores prácticas.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	100% Meta Constante	$1.199	$ 3.308





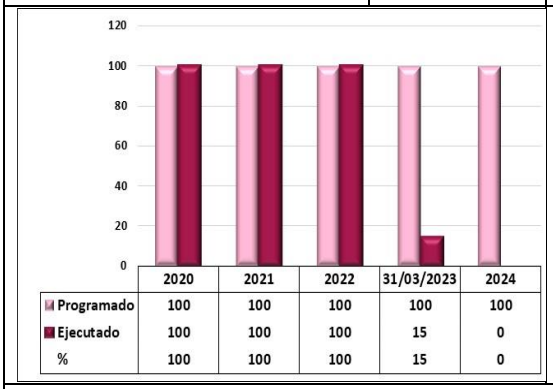
Análisis OCI: Teniendo en cuenta los datos registrados en SEGPLAN con corte a 31/03/2023, se pudo determinar una ejecución de la magnitud del 15% soportado en el ajuste del procedimiento de uso y apropiación, gestión de incidentes o problemas y eliminación del procedimiento gestión de incidentes.

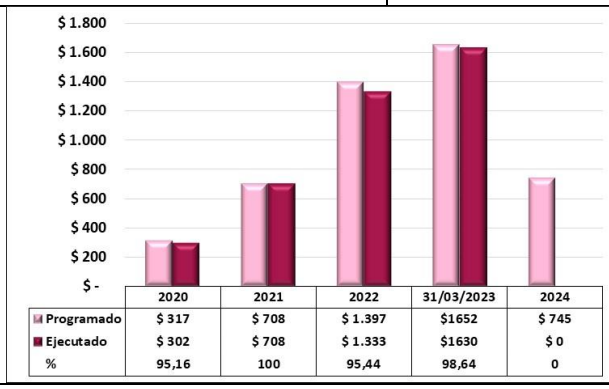
En lo referente a la ejecución presupuestal se observó un total comprometido del 100% y un giro acumulado de $66.458.516 lo cual corresponde al 6% de lo comprometido con corte a 31/03/2023.

*Tabla N°11. Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023. Nota: *Cifras Millones de pesos.*

- **Meta 7 Planear y ejecutar al 100 por ciento la estrategia de actualización de los sistemas de información existente e implementación de nuevos, con el fin de mejorar su funcionalidad, accesibilidad y usabilidad, acorde a los procesos y procedimientos que hacen parte del mapa de procesos de la Entidad.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	100% Meta Constante	$1.652	$ 4.820





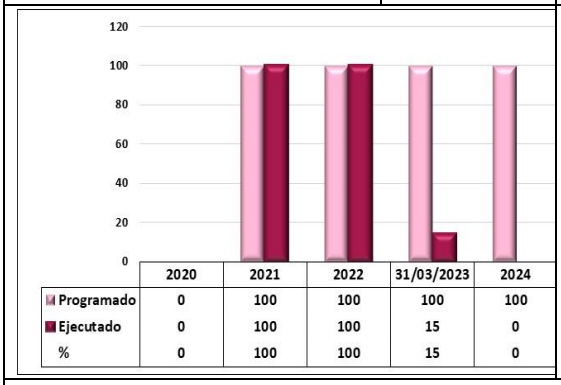
Análisis OCI: Teniendo en cuenta los datos registrados en SEGPLAN con corte a 31/03/2023, se pudo determinar una ejecución de la magnitud del 15% soportado en mesas de trabajo con el objetivo de revisar los sistemas de información con las áreas funcionales.

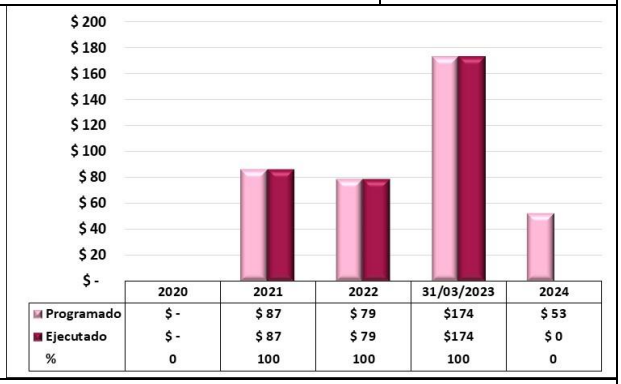
En lo referente a la ejecución presupuestal se observó un total comprometido del 98,64% y un giro acumulado de $61.709.128 lo cual corresponde al 4% de lo comprometido con corte a 31/03/2023.

*Tabla N°12.Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023. Nota: *Cifras Millones de pesos.*

- **Meta 8 Planear y ejecutar al 100 por ciento la estrategia para fortalecer el uso y apropiación de los servicios tecnológicos al interior de la Entidad, mediante acciones continuas de sensibilización y/o capacitación.**

Magnitud		Recursos	
Meta Vigencia 2023 Corte 31/03/2023	**Meta Cuatrienio**	**Presupuesto Vigencia Corte 31/03/2023**	**Presupuesto Cuatrienio**
100%	100% Meta Constante	$ 174	$ 394





Análisis OCI: Teniendo en cuenta los datos registrados en SEGPLAN con corte a 31/03/2023, se pudo determinar una ejecución de la magnitud del 15% soportado en mesas de trabajo para el fortalecimiento de los servicios ciudadanos digitales, publicación de piezas de comunicación referente a SIGA, Factor de autenticación, seguridad de la información, gestión de cambios entre otras.

En lo referente a la ejecución presupuestal se observó un total comprometido del 100% y un giro acumulado de $9.383.333 lo cual corresponde al 5% de lo comprometido con corte a 31/03/2023.

*Tabla N°13. Elaboración Propia. Fuente: Plan de Acción 2020-2024 componente de inversión Corte 31/03/2023 Nota: *Cifras Millones de pesos.*

La Reserva Definitiva del proyecto de inversión 7777 con corte a 31 de marzo de 2023 corresponde a un valor de $ 3.147.018.071 con una autorización de giro de $ 1.227.756.699 equivalente al 39%.

El proyecto relacionado a cierre del primer trimestre de 2023 registra un valor de Pasivos Exigibles sin proceso judicial de $ 90.438.088, sin presentar pagos ni depuraciones.

En conclusión, el proyecto de inversión 7777, con corte a 31/03/2023, realizó un avance en un rango de ejecución física entre el 15% y 24%, así como un compromiso entre el 10% y 100% y un giro presupuestal entre el 2% y 6%.

Es importante tener en cuenta que esta información está sujeta a cambios y actualizaciones posteriores al periodo objeto de evaluación, por lo tanto, se recomienda realizar seguimientos periódicos a las reservas y pasivos exigibles del proyecto con el objetivo de tomar las medidas necesarias para su pago o depuración asegurando una adecuada gestión financiera para su utilización efectiva.

3.4 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI

Generalidades del PETI:

De acuerdo con lo establecido en la Resolución 004 del 2017 y en concordancia con el Decreto 415 de 2016, esta oficina validó la implementación y seguimiento a la ejecución del Plan Estratégico de

Tecnologías de la información por parte del proceso de Gestión de Tecnologías de la Información, de acuerdo con los siguientes criterios:

1. Alineación del PETI con la estrategia y Modelo Integrado de Planeación y Gestión MIPG de la Entidad.[5]
2. Gestión, Seguimiento y Control de la ejecución de los recursos financieros asociados al portafolio de proyectos y servicios definidos en el PETI.[6]
3. Seguridad Digital; adoptar las políticas de protección y mitigación que resulten pertinentes a sus necesidades.[7]
4. Adopción de políticas de seguridad, custodia de los datos e información y establecer los procedimientos para el adecuado uso y administración de los recursos informáticos.[8]
5. Cumplimiento de la Ley de Transparencia y la normatividad Gobierno en Línea.[9]

El equipo auditor, a través de mesa de trabajo el día 14 de junio de 2023 con los profesionales responsables del PETI procedió a validar el documento "Plan Estratégico de Tecnologías de la Información 2020-2024", obteniendo los siguientes resultados:

Criterio	Validación OCI
Alineación del PETI con la estrategia y Modelo Integrado de Planeación y Gestión MIPG de la Entidad	Se identificó que dentro del documento PETI que en los numerales 6.6. y numeral 7 su alineación con el Modelo Integrado de Planeación y Gestión MIPG y el modelo de operación por procesos de la SDSCJ según corresponde. No obstante, al validar la información registrada en el PETI en el numeral 10, se encontraron diferencias e información desactualizada entre la información contenida en el sistema de gestión de calidad (Portal MIPG) y lo enunciado en el documento; en los siguientes ítems: Políticas, Procedimientos e Indicadores del proceso TICS.
Gestión, Seguimiento y Control de la ejecución de los recursos financieros asociados al portafolio de proyectos y servicios definidos en el PETI	Se verificó que el PETI incluye en el numeral 12 un portafolio de iniciativas en el marco del proyecto de inversión 7777 con el registro de proyecciones financieras para el periodo de 2020-2024. En mesa de trabajo se validó con los profesionales de TICS que el seguimiento y control de la ejecución de los recursos financieros de las iniciativas se realiza a través de SEGPLAN.
Seguridad Digital; adoptar las políticas de protección y mitigación que resulten pertinentes a sus necesidades	Se identificó que el PETI describe el proyecto de inversión 7777 *"Fortalecimiento de la gestión de las Tecnologías de la Información en la Secretaría de Seguridad, Convivencia y Justicia en el marco de las políticas de gobierno y seguridad digital en Bogotá",* en el cual, uno de sus objetivos es fortalecer la oferta de servicios ciudadanos digitales que ofrece la Entidad, así como la publicación en el Portal MIPG de la Política de Seguridad y Privacidad de la Información PO-GT-1- V5.
Adopción de políticas de seguridad, custodia de los datos e información y establecer los procedimientos para el adecuado uso y administración de los recursos informáticos	Dentro del documento PETI se contempla y desarrolla los lineamientos en Seguridad y Privacidad en la Información en su numeral 9.8, adicional la Entidad adoptó la Política de Seguridad y Privacidad de la Información PO-GT-1- V5.

[5] Artículo 2.2.35.3 Numeral 1 del Decreto 415 de 2106.
[6] Artículo 2.2.35.3 Numeral 4 del Decreto 415 de 2106.
[7] Artículo 5 de la Resolución 004 de 2017.
[8] Artículo 6 de la Resolución 004 de 2017.
[9] Artículo 8 de la Resolución 004 de 2017.

Criterio	Validación OCI
Cumplimiento de la Ley de Transparencia y la normatividad Gobierno en Línea	Se identificó que el PETI se encuentra publicado en la Página web de la Entidad https://scj.gov.co/sites/default/files/planeacion/PL-GT-2_V4.pdf en su versión 4 del 31 de enero de 2023, así como en el Portal MIPG para su consulta. No obstante, no se logró evidenciar dentro del documento del PETI donde se relaciona la aplicación de la normatividad de gobierno en línea.

Tabla N°14. Elaboración Propia. Fuente: Plan Estratégico de Tecnologías de la Información PETIC 2018-2020 PL-GT-2 - versión 4

Como resultado de esta validación, se concluye que el documento PETI contiene los elementos referidos en la normatividad vigente, no obstante, dicho documento debe estar actualizado en lo referente a políticas, procedimientos e indicadores que actualmente el proceso de Gestión de Tecnologías de la Información tiene adoptados en el Sistema Integrado de Gestión y por otra parte, desarrollar la Política de Seguridad Digital en la entidad de acuerdo a los lineamientos que establece el Decreto 767 de 2022 sección 2 articulo 2.2.9.1.2.1. emitido por la Presidencia de la Republica.

OBSERVACIÓN N° 3: Ausencia de un documento que desarrolle la Política de Seguridad Digital en la Entidad, para dar cumplimiento a la normatividad vigente:
El PETI 2020-2024 de acuerdo con la Resolución 004 del 2017 debe estar alineado con las políticas en materia de TIC, una de ellas es la Política de Seguridad Digital y Gobierno Digital; la cual se identificó en el documento "*Política de Seguridad y Privacidad de la Información PO-GT-1*" versión 5 adoptada y publicada en el Portal MIPG, que describe en su introducción y objetivo "*orientar a la entidad al cumplimiento de las directrices nacionales frente a Seguridad Digital y Gobierno Digital*", sin embargo, no se evidenció dentro de dicho documento el cumplimiento o aplicación de los lineamientos del Decreto 767 de 2022 sección 2 articulo 2.2.9.1.2.1. en lo referente al desarrollo de los elementos a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras.

RECOMENDACIÓN N° 5: Adelantar las acciones al interior del proceso, que conlleven a documentar y oficializar la Política de Seguridad Digital en la Entidad en lo referente a los elementos que establece el Decreto de la Presidencia número 767 de 2022 sección 2 articulo 2.2.9.1.2.1.

Validación metodológica del PETI:

En la verificación del PETI 2020-2024 se tomó como fuente de información el documento "*Plan Estratégico de Tecnologías de la Información PETIC 2018-2020 PL-GT-2*" versión 4 publicada en el Portal MIPG, encontrando inconsistencia en el título del documento con relación a la vigencia del plan (2018-2020), siendo el periodo correcto (2020-2024)

La información contenida en documento fue cotejada con los entregables propuestos en la *Guía para la construcción del PETI versión 2019 elaborada por el Ministerio de Tecnologías de la Información y las Comunicaciones* y de acuerdo con la información suministrada por el proceso el día 27 de junio de 2023 mediante correo electrónico. A continuación, se presentan las siguientes situaciones:

Guía PETI v2.0 2019		PETI SDSCJ 2020-2024		Observaciones OCI
SECCIÓN	EVIDENCIA	Información enviada por TICS 27-06-2023	Numeral validado	
Marco Normativo	Marco Normativo	Numeral 5	Numeral 5	El vínculo del enlace no funciona y no se encontró la normatividad asociada al plan.
Principios de la Transformación Digital	Principios de la Transformación Digital	No enviada por TICS	Sin validar	No se encontró la sección en el PETI 2020-2024
Misión de TI	Misión de TI	No enviada por TICS	Sin validar	No se encontró la sección en el PETI 2020-2024
Objetivos institucionales	Objetivos institucionales	No enviada por TICS	Sin validar	No se encontró la sección en el PETI 2020-2024
Uso y apropiación	Análisis DOFA	Numeral 10.6	No validado	En el **numeral 10.6** no se encontraron relacionadas las debilidades, oportunidades, fortalezas y amenazas para el uso y apropiación de la política.
Sistemas de Información	Catálogo de hallazgos	Numeral 10.4	Sin validar	**En los numerales 10.2, 10.3, 10.4 y 10.5** no se relaciona el catálogo de hallazgos (id del servicio, descripción del hallazgo, impacto, evidencia, URL), de acuerdo con lo establecido en la Guía para la construcción del PETI emitida por Min Tic
Análisis financiero	Iniciativas asociadas a la operación	Numeral 12	Sin validar	No se encontró la sección en el PETI 2020-2024
Estrategia de TI - Objetivos de TI	Objetivos de TI Objetivos de TI vs Objetivos de la Entidad	No enviada por TICS	Sin validar	No se encontró la sección en el PETI 2020-2024
Gobierno de TI	Gobierno de TI	Numeral 10.1.3	Numeral 9.3	La información se validó en la sección 9.3
Modelo de gestión de servicios tecnológicos	Modelo de gestión de servicios tecnológicos	Numeral 7	Numeral 10	**En el numeral 10.1.3** se menciona *"se espera realizar la actualización de la estructura organizacional con la que espera funcionar durante esta vigencia*", no obstante, el proceso confirmó que no se va a realizar dicha actualización, lo cual no es coherente con la redacción del numeral. **En el numeral 10.1.4** No se encontraron las políticas relacionadas en el numeral debidamente adoptadas por el proceso en el portal MIPG. **En el numeral 10.1.5** En relación a la documentación relacionada, no se contó con un porcentaje de avance para su

Guía PETI v2.0 2019		PETI SDSCJ 2020-2024		Observaciones OCI
SECCIÓN	EVIDENCIA	Información enviada por TICS 27-06-2023	Numeral validado	
				actualización, el proceso informó que continúan realizando ajustes a los documentos. **En el numeral 10.1.7** los indicadores relacionados no corresponden a los activos para el proceso en el Portal MIPG. Adicionalmente, el proceso aportó las hojas de vida de la vigencia 2022 relacionando únicamente los indicadores de gestión activos en el portal, pero no los descritos en el numeral. **En el numeral 10.1.8** El enlace del tablero de control relaciona únicamente los indicadores de gestión, sin embargo, no se evidenció información relacionada con el seguimiento de los objetivos y metas establecidos por la DTSI, para así contar con una vista resumida de lo que está ocurriendo en las diferentes áreas en cuanto a tecnologías de la información.

Tabla N°15. Elaboración Propia. Fuente: Plan Estratégico de Tecnologías de la Información PETIC 2018-2020 PL-GT-2 - versión 4

OPORTUNIDAD DE MEJORA N° 3: Debilidades en el documento PETI, respecto a la guía para la construcción emitida por MINTIC:

El Plan Estratégico de Tecnologías de la Información PETIC 2020-2024 - versión 4 no se encontró alineado en su totalidad con la *Guía para la construcción del PETI versión 2019 elaborada por el Ministerio de Tecnologías de la Información y las Comunicaciones* y se identificó información desactualizada en los numerales 10.1.3, 10.1.4, 10.1.5, 10.1.7 y 10.1.8. de acuerdo con las validaciones realizadas en el Portal MIPG y la Página web de la Entidad.

RECOMENDACIÓN N° 6: Ajustar, adoptar y socializar el documento *Plan Estratégico de Tecnologías de la Información PETIC 2018-2020 PL-GT-2,* teniendo en cuenta los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones y los instrumentos de gestión del proceso.

3.5 REVISIÓN DE PROCEDIMIENTOS ASOCIADOS AL PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

El equipo auditor que desarrolló el ejercicio de revisión y validación al proceso Gestión de Tecnologías de la Información, seleccionó aleatoriamente procedimientos para auditar equivalentes al 75 por ciento del total; a continuación, se presenta el detalle de los procedimientos auditados:

Procedimiento	Auditado
Gestión de Requerimientos de TI PD-GT-1	Si
Gestión de Cambios de TIC PD-GT-2	Si
Gestión de proyectos de TI PD-GT-4	Si
Procedimiento Gestión de Incidentes o Problemas PD-GT-6	Si
Administración de Usuarios PD-GT-8	Si
Gestión de infraestructura y plataformas tecnológicas PD-GT-11	Si
Control de Acceso a Plataformas PD-GT-12	Si
Procedimiento de uso y apropiación PD-GT-13	No
Gestión de Requerimientos Tecnológicos PD-GT-15	No
Gestión de Pruebas Tecnológicas PD-GT-16	No
Ciclo de Vida de Desarrollo de Software PD-GT-17	Si
Gestión de Datos Abiertos PD-GT-18	Si

Tabla N°16. Elaboración propia.

Una vez culminado el trabajo de campo por parte del equipo auditor, se obtienen las siguientes observaciones y oportunidades de mejora evidenciadas por cada uno de los procedimientos:

3.5.1 PD-GT-1 Procedimiento Gestión de Requerimientos de TI Versión 6

Una vez revisada la estructura del procedimiento *"Gestión de Requerimientos de TI - PD-GT-1-V-6"* se pudo determinar que:

- El objetivo y el alcance del procedimiento son amplios, no establecen claramente el propósito de este, no proporcionan detalles suficientes sobre las solicitudes de servicios tecnológicos lo que genera confusiones con el procedimiento "*Gestión de Requerimientos Tecnológicos* PD-GT- 15 versión 4.

- Si bien en las políticas de operación describen diferentes tipos de solicitudes de servicios Tecnológicos, esta clasificación no se encuentra en el reporte generado de la herramienta de gestión, por lo tanto, no es posible verificar la clasificación de las solicitudes por tipología.

- El procedimiento no establece plazos o tiempos de respuesta (SLA – Acuerdos de niveles de servicio) para atender las solicitudes de servicio tecnológico por lo cual no es posible determinar la eficiencia y la oportunidad en la atención de los requerimientos.

- Puntos de Control: Respecto a los puntos de control, se determinó que estos permiten verificar el cumplimiento de las actividades establecidas, siendo relevantes para la atención y gestión de las solicitudes.

Validación del Procedimiento:

Para la validación del procedimiento *"Gestión de Requerimientos de TI - PD-GT-1-V-6"* se tomó como fuente de información el archivo *"Requerimientos.xlsx"* suministrado por parte del proceso auditado mediante correo electrónico del 13 de junio de 2023, este cuenta con un total de 17.031 registros del periodo comprendido entre el 1 de enero de 2022 al 30 de abril de 2023 distribuidos de la siguiente forma:

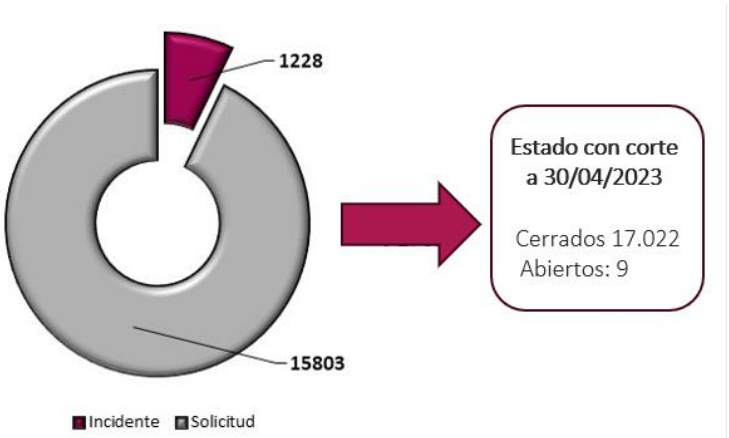


Imagen N°01. Tipo de Caso y estado de Requerimientos - Elaboración propia OCI – Fuente: Archivo "Requerimientos.xlsx"

Así las cosas, se tuvieron en cuenta los siguientes criterios para la obtención de la muestra:

INGRESO DE PARÁMETROS	
Tamaño de la Población (N)	17.031
Error Muestral (E)	10%
Proporción de Éxito (P)	10%
Nivel de Confianza	90%
Nivel de Confianza (Z) (1)	1,645

Tabla N°17. Elaboración Propia OCI – Anexo 7 Caja de Herramientas – Guía de Auditoria Basada en Riesgos para Entidades Publicas

Con base en estos criterios, se procedió a calcular el tamaño de la muestra con un resultado de 24 registros. Según los criterios mencionados y registros evaluados, se pueden concluir lo siguiente:

- Numeración asignada: El 100% de los casos cuentan con un número asignado en la herramienta de gestión definida por la Entidad. Esto indica que todos los registros fueron debidamente identificados y clasificados.

- Solicitud a través de canales dispuestos: Los 24 casos verificados muestran que todas las solicitudes fueron realizadas utilizando los diferentes canales disponibles por parte de la Entidad. Esto asegura que los usuarios aplican los medios establecidos para presentar sus solicitudes.

- Gestión de seguimiento: El 100% de las solicitudes registran una gestión de seguimiento por parte de los colaboradores designados por la Dirección de Tecnología de Información. Esto significa que se llevó un control y seguimiento de las solicitudes para su debida atención y resolución.

- Uso de formatos relacionados con el procedimiento: De los 24 casos evaluados, en aquellos en los que aplicaba el uso de formatos 10 de estos contaban con los formatos establecidos en el procedimiento en temas relacionados con: préstamo de elementos, creación de

usuarios y concepto técnico, por lo tanto, estos fueron debidamente documentados en los registros correspondientes. Sin embargo, para los Conceptos Técnicos de Elementos de Tecnología F-GT-422 de las solicitudes SR206893, SR200841 no se cuenta con datos ni firma de quien recibe el equipo y/o concepto.

En resumen, los resultados obtenidos de la muestra indican un cumplimiento del 100% en los aspectos evaluados, lo cual sugiere que los registros analizados cumplen con los requisitos establecidos por la Entidad en términos de numeración, canales de solicitud y gestión de seguimiento.

Tiempos de cierre de Solicitudes:

Para la verificación de tiempos de cierre de las solicitudes en la mesa de servicio, se tomó como insumo el archivo *"Requerimientos.xlsx" y* se realizó cálculo de los días calendario de respuesta de los 17.022 requerimientos en estado cerrado como se detalla a continuación:

Rango de Días Calendario de Cierre	Numero de Solicitudes	%
0 - 5 días	14169	**83,24%**
6 - 15 días	2191	**12,87%**
16 - 30 días	301	**1,77%**
Mayor a 30 días	360	**2,11%**
Sin Fecha de Cierre	1	**0,01%**
Total	17022	**100,00%**

Tabla N°18. Rango de días Cierre solicitudes en la mesa de servicio - Elaboración propia OCI – Fuente: Archivo "Requerimientos.xlsx"

Como resultado de la prueba se pudo determinar que:

- El 83,24% de las solicitudes se cierran en un rango de 0 a 5 días, y que el 2,11% se cierran en la mesa de servicios en un tiempo mayor a 30 días.

- Durante la entrevista realizada el viernes 16 de junio de 2023 a través de la plataforma Teams, se constató que la fecha de cierre en la mesa de servicio presentada en el reporte generado de la herramienta Service Manager, no siempre coincide con la fecha en la cual se realizó la gestión para resolver el requerimiento. Esto revela una debilidad en el procedimiento, ya que no se establece un tiempo máximo de cierre por parte del colaborador designado.

- Por otra parte, en el archivo *"Requerimientos.xlsx"* no se pudo identificar clasificación y/o tipología lo cual limita la capacidad de verificar si el tiempo de cierre de las solicitudes en la mesa de servicio es eficiente y oportuno de acuerdo con el tipo de requerimiento.

Encuestas de satisfacción:

Como parte de la auditoría, se procedió a validar las encuestas diligenciadas por los usuarios durante el periodo comprendido entre el 1 de enero de 2022 y el 1 de mayo de 2023, en relación con la actividad 9 del procedimiento PD-GT-1, que establece *"Analizar evaluación de satisfacción"* y su

registro correspondiente *"Relación con los resultados de las encuestas de satisfacción"*. La encuesta cuenta con un total de 4 preguntas, de las cuales tres miden la satisfacción, a continuación, se relacionan y se presentan los resultados:

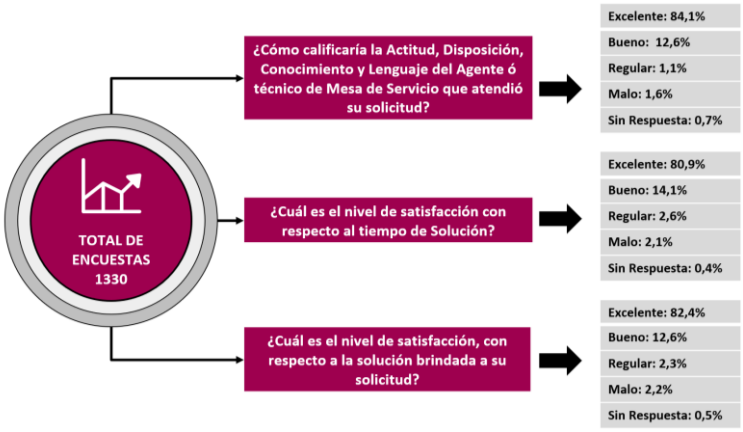


Imagen N°02. Resultados Encuestas de Satisfacción - Elaboración propia OCI – Fuente: Archivo "Encuestas.xlsx"

Respecto a los resultados relacionados con el nivel de satisfacción este se encuentra entre el 80,9 y el 84,1% calificando como excelente el servicio recibido.

Sin embargo, al analizar la implementación de la actividad 9 del procedimiento, se observa una discrepancia entre lo descrito en la actividad y la salida (registro) establecida. La actividad 9 indica la necesidad de realizar una revisión y análisis de las encuestas de satisfacción para identificar oportunidades de mejora. No obstante, la única salida registrada es "R*elación con los resultados de las encuestas de satisfacción*", lo cual no refleja de manera adecuada el análisis realizado por el proceso. Esto indica una falta de coherencia en el registro establecido para la actividad.

Además, se identifica que la actividad 9 no específica una periodicidad para su ejecución, lo que dificulta asegurar una revisión y análisis periódico de las encuestas de satisfacción.

OBSERVACIÓN N° 4 Debilidades en la Elaboración y Control del Procedimiento "Gestión de Requerimientos de TI - PD-GT-1-V-6":

El equipo auditor reporta debilidades en la elaboración del procedimiento *"Gestión de Requerimientos de TI - PD-GT-1-V-6" respecto* a la descripción de la entrada o insumo de la Actividad N°2, así como la descripción de la Actividad N°9 y el registro de salida. De igual manera, falta de claridad en el objetivo y el alcance generando confusiones versus el procedimiento *"Gestión de Requerimientos Tecnológicos* PD-GT- 15 versión 4. Lo anterior, denota falencias en la información y/o documentación a cargo del proceso, como se encuentra señalado en la Guía de *"Elaboración y Control de Documentos del Sistema de Gestión".*

RECOMENDACIÓN N° 7: Revisar y corregir las debilidades identificadas en el procedimiento *"Gestión de Requerimientos de TI - PD-GT-1-V-6"*, lo anterior, permitirá mejorar la calidad y coherencia del documento, cumpliendo con los requisitos establecidos en la Guía de *"Elaboración y Control de Documentos del Sistema de Gestión".*

OPORTUNIDAD DE MEJORA N° 4: Documentar y Estandarizar Tiempos de Respuesta y Cierre de Solicitudes de Servicio Tecnológico:
Una vez verificado el procedimiento, se observó que este no establece plazos o tiempos de respuesta para atender las solicitudes de servicio tecnológico por lo cual no es posible determinar la eficiencia y la oportuna atención de los requerimientos.

RECOMENDACIÓN N° 8: Estandarizar los tiempos de respuesta de acuerdo con la tipología estableciendo tiempos máximos de cierre de las solicitudes en la herramienta de gestión y así contribuir a una gestión eficiente y oportuna de los requerimientos de servicios tecnológicos.

3.5.2 PD-GT-2 Procedimiento Gestión de Cambios TIC Versión 5:

El equipo auditor procedió a validar el uso de los formatos vigentes dentro del sistema integrado de gestión, encontrando para este procedimiento lo siguiente:

Actividad	Formato	Validación 2022	Validación 2023
Actividad N° 1 Realizar la solicitud de cambio	Formato gestión de cambios - F-GT-278	El proceso aportó un total de 81 solicitudes de gestión de cambios para la vigencia 2022. Frente a lo evaluado se encontraron ocho (8) solicitudes de gestión de cambios tramitadas con versiones anteriores a la publicada en el portal MIPG (v4 del 13 de marzo del 2020). Adicionalmente, se encontró el uso de un archivo de Excel con el seguimiento y control de los cambios solicitados y efectuados, el cual no se encuentra dentro del portal MIPG como un documento oficial del proceso.	El proceso aportó 18 solicitudes de gestión de cambios para la vigencia 2023. Frente a lo evaluado se encontraron seis (6) solicitudes de gestión de cambios tramitadas con versiones anteriores a la publicada en el portal MIPG (v4 del 13 de marzo del 2020) Adicionalmente, se encontró el uso de un Excel con el seguimiento y control de los cambios solicitados y efectuados, el cual no se encuentra dentro del portal MIPG como un documento oficial del proceso.
Actividad N° 9 Realizar pruebas del cambio	Formato bitácora de actividades - F-GT-277	El proceso aportó un total de 78 bitácoras de la vigencia 2022. Frente a lo evaluado se encontraron seis (6) bitácoras sin firmas y nueve (9) firmadas parcialmente.	El proceso aportó 15 bitácoras de la vigencia 2023. Frente a lo evaluado se encontraron cuatro (4) bitácoras firmadas parcialmente.
Actividad N° 6 Realizar el comité de gestión de cambios	Acta de reunión Comité de Gestión de cambios	El proceso no aportó evidencia de actas de reunión del comité de gestión de cambios para la vigencia 2022.	El proceso no aportó evidencia de actas de reunión del comité de gestión de cambios para la vigencia 2023.

Tabla N°19. Elaboración Propia. Fuente: PD-GT-2 Versión 5 Procedimiento Gestión de Cambios TIC

OBSERVACIÓN N° 5: Debilidades en el uso y aplicación de los formatos establecidos en el procedimiento Gestión de Cambios TIC PD-GT-2 - Versión 5:
El equipo auditor evidenció debilidades en el uso de los soportes documentales establecidos en el procedimiento PD-GT-2 Gestión de cambios TIC, al encontrar en el uso del formato "Gestión de

cambios - F-GT-278" en versiones anteriores a la adoptada desde el 13 de marzo de 2020 (v4); de igual manera el formato "Bitácora de actividades - F-GT-277" sin firmas y no se cuenta con el diligenciamiento de las actas de reunión del Comité de Gestión de Cambios. Lo informado denota falencias en lo establecido en el sistema integrado de gestión de la Entidad.

RECOMENDACIÓN N° 9: Actualizar el procedimiento PD-GT-2 Gestión de cambios TIC, en el cual se verifiquen y confirmen los formatos a utilizar en el desarrollo de este y complementariamente generar controles asociados para garantizar el correcto uso y aplicación de los formatos vigentes en el Portal MIPG de la Entidad.

Durante el ejercicio auditor se inició con la verificación de los puntos de control asociados al procedimiento en mención, obteniendo dos aspectos por mejorar:

Punto de control	¿se encuentra redactado como un punto de control? SI/NO	¿Se establece responsable? SI/NO	¿Se establece evidencia? SI/NO	Verificación OCI
Actividad n° 6 Verificar que se cumplan las políticas de operación de cambios y la cantidad de votos requerida para aprobar el cambio.	SI	NO	SI	El proceso no aportó las actas de comité de gestión de cambios para la vigencia 2022 y 2023, lo cual no permitió verificar la aplicación del control. En reunión con el proceso el día 30 de mayo de 2023 se identificó que la aprobación realizada en el comité se documenta en el formato Gestión de Cambios - F-GT-278.
Actividad n° 9 Bitácora de actividades F-GT-277	NO	NO	SI	Al verificar el punto de control, esté no se encuentra redactado adecuadamente al mencionarse únicamente un formato y no especificar la acción de control.

OBSERVACIÓN N° 6: Falencia en el diseño de puntos de control del procedimiento Gestión de Cambios y en su aplicación:
En el proceso de revisión ejecutado por el equipo auditor, se observó que no se cuenta con las actas de comité de gestión de cambios del periodo comprendido entre el 01 de enero de 2022 hasta el 31 de marzo de 2023, el cual garantiza la correcta aplicación del punto de control N° 6 "*Verificar que se cumplan las políticas de operación de cambios y la cantidad de votos requerida para aprobar el cambio.*" contemplado dentro del procedimiento PD-GT-2 Procedimiento Gestión de Cambios TIC.

RECOMENDACIÓN N° 10: Revisar y ajustar los puntos de control asociados al procedimiento, con el fin de guardar coherencia con la actividad y como medidas de control eficaz para reducir la probabilidad de desviación.

3.5.3 PD-GT-4 Procedimiento Gestión de Proyectos Versión 5:

Una vez revisada la estructura del procedimiento *"Gestión de proyectos de TI - PD-GT-4-V5"* se pudo determinar que:

- El objetivo y el alcance se alinean con el propósito general del proceso.

- Los puntos de control se han establecido para evaluar la viabilidad de una solicitud de solución tecnológica y verificar la información actualizada del requerimiento como se describe a continuación:

- Punto de Control 7: *"Solicitud de solución tecnológica F-GT-192 diligenciado Acta(s) de reunión de alcance de requerimiento"* En este punto de control, se realiza un análisis de viabilidad jurídica, financiera y técnica basado en la información proporcionada en la solicitud de solución tecnológica y en las actas de reunión de alcance de requerimiento. Se verifica la completitud, consistencia y pertinencia de los datos consignados. Si la solicitud no es viable, se informa al solicitante por correo electrónico y se brindan explicaciones sobre las razones de dicha decisión, junto con posibles recomendaciones de alternativas de solución, por lo tanto, el punto de control establecido asegura el análisis de la viabilidad del proyecto.

- Punto de Control 11: "Solicitud de solución tecnológica F-GT-192 actualizado"
  En este punto de control, se verifica la información actualizada del requerimiento para asegurarse de que esté completa, consistente y pertinente con el alcance de este. Se realiza una revisión de la solicitud de solución tecnológica, y si es necesario, se pueden realizar observaciones o actualizaciones en el requerimiento registrado en la mesa de servicio. Sin embargo, no se documentan puntos de control con el propósito de asegurar la ejecución y cierre del proyecto.

- Los registros de salida en las actividades no cuentan con la relación de los formatos soporte, así mismo, el formato Valoración de complejidad del proyecto, F-GT-930 pese a encontrarse relacionado en los documentos de referencia y en las políticas de operación no se encuentra relacionado en las actividades del procedimiento en mención.

Validación del procedimiento:

- En concordancia con lo establecido en las políticas de operación del "Dominio Legal" la SDSCJ cuenta con un Portafolio de Proyectos en el Plan Estratégico de tecnologías de la Información PETI numeral 13. En este se registran un total de 15 proyectos en el siguiente estado:

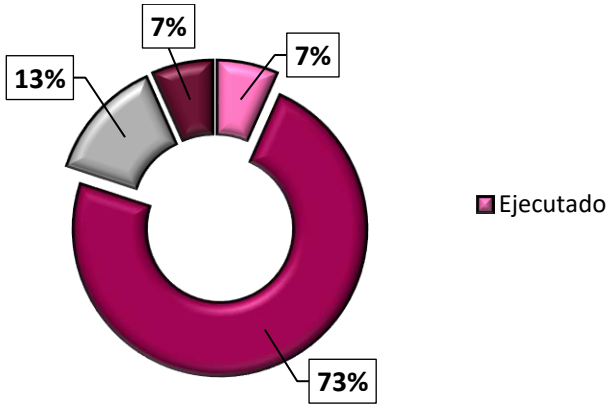


Imagen N°03. Estado Proyectos Elaboración propia OCI – Fuente: "Archivo Excel Base de datos Estados de proyectos DTSI 2023"

De acuerdo con la política de operación: *"…En la Secretaria Distrital de Seguridad, Convivencia y Justicia, de acuerdo a lo definido en el presente procedimiento para la Administración y Gestión de proyectos TI, se debe diligenciar como mínimo los siguientes formatos: 1. Valoración de complejidad del proyecto, F-GT-930, 2. Acta de inicio/Constitución del proyecto, F-GT-544 3. Acta entrega y recibo a satisfacción de entregable(s) /producto(s) del proyecto, F-GT-927 4. Acta de terminación y cierre del proyecto, F-GT-648, 5. Plan General del proyecto, F-GT-935, 6. Reporte de ejecución y control del proyecto, F-GT-936, 7. Portafolio de proyectos, F-GT-931 ..."* se procedió a verificar los documentos aportados por el proceso encontrando:

Dependencia o Proceso	Proyecto	Porcentaje de Ejecución I trimestre 2023	FECHA DE INICIO	FECHA DE FINALIZACION	Seguimiento
Despacho	Implementación Herramienta de Seguimiento a compromisos - Despacho	100%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Solicitud F-GT-192 del 29/03/2023, 27/05/2923 y 22/04/2023 Acta de inicio/Constitución del proyecto, F-GT-544. - No se observan los siguientes formatos Valoración de complejidad del proyecto, F-GT-930. Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936 Acta entrega y recibo a satisfacción de entregable(s) /producto(s) del proyecto, F-GT-927 Acta de terminación y cierre del proyecto, F-GT-648

Dependencia o Proceso	Proyecto	Porcentaje de Ejecución I trimestre 2023	FECHA DE INICIO	FECHA DE FINALIZACION	Seguimiento
Fortalecimiento Acceso a la Justicia	Sistema de turnos	90%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Solicitud F-GT-192 del 21/05/2021 (Sin número de Ticket, sin firmas). - No se observan los siguientes formatos: Valoración de complejidad del proyecto, F-GT-930. Acta de inicio/Constitución del proyecto, F-GT-544. Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936 Es importante precisar, que pese a que la solicitud del formato F-GT-192 tiene fecha anterior a la vigencia del procedimiento, el inicio del desarrollo tiene fecha posterior a esta, por lo tanto, aplica la versión 5 del procedimiento objeto de auditoría.
Fortalecimiento de capacidades operativas	SIMBA FASE II	8%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Solicitud F-GT-192 del 21/09/2020 - Acta de inicio/Constitución del proyecto, F-GT-544.en elaboración -No se observan los siguientes formatos: Valoración de complejidad del proyecto, F-GT-930. Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936
Gestión de comunicaciones	Rediseño del sitio Web	20%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Solicitud F-GT-192 del 28/10/2019 - Ticket SR55252 y SR55254. Acta de inicio/Constitución del proyecto, F-GT-544. (no se encuentran diligenciado los numerales 2,3 variable tiempo, 3,2 Presupuesto Requerido, 5, Aprobación y Formalización del Proyecto, 6, Control de Elaboración /Revisión/Aprobación del Acta) Valoración de complejidad del proyecto, F-GT-930. - No se observan los siguientes formatos: Plan General del proyecto, F-GT-935. (Si bien se adjunta formato, este no se encuentra diligenciado) Reporte de ejecución y control del proyecto, F-GT-936 Es importante precisar, que pese a que la solicitud del formato F-GT-192 tiene fecha anterior a la vigencia del procedimiento, el inicio del desarrollo tiene fecha posterior a

Dependencia o Proceso	Proyecto	Porcentaje de Ejecución I trimestre 2023	FECHA DE INICIO	FECHA DE FINALIZACION	Seguimiento
					esta, por lo tanto, aplica la versión 5 del procedimiento objeto de auditoría.
Gestión de Emergencias	Convergencia tecnológica de sistemas técnicos de apoyo	No Ejecución	No ejecución	No ejecución	Se manifiesta por la DTSI que el formato F-GT-192 no aplica, teniendo en cuenta que la iniciativa solo se dio la etapa de prefactibilidad, la cual no se encuentra documentada en el procedimiento. Se evidencia - Concepto Técnico Favorable, el cual se entregó mediante Formato F-FC-742 de fecha 29 de septiembre de 2022, así mismo, se informa que "por parte de C4 no se surtieron las fases posteriores del proyecto y a la fecha se informa por el área desde donde se originó la necesidad o iniciativa, que no hay recursos para adelantar el proyecto en la presente vigencia"
	Migración del Data Center	No Ejecución	No ejecución	No ejecución	Se manifiesta por la DTSI que el formato F-GT-192 no aplica, teniendo en cuenta que la iniciativa solo se dio la etapa de prefactibilidad, la cual no se encuentra documentada en el procedimiento. Se evidencia - Concepto Técnico Favorable, el cual se entregó mediante Formato F-FC-742 de fecha 20 de septiembre de 2022, así mismo, se informa que "Por parte de C4 no se surtieron fases posteriores del proyecto y a la fecha se informa por el área desde donde se originó la necesidad o iniciativa, que no hay recursos para adelantar el proyecto en la presente vigencia."

Dependencia o Proceso	Proyecto	Porcentaje de Ejecución I trimestre 2023	FECHA DE INICIO	FECHA DE FINALIZACION	Seguimiento
	Registro Sistemas de Video vigilancia (acuerdo 815)	97%	1/01/2022	31/12/2022	-Se evidencian los siguientes Formatos:Solicitud F-GT-192 del 10/02/2023.Valoración de complejidad del proyecto, F-GT-930.Acta de inicio/Constitución del proyecto, F-GT-544.Acta entrega y recibo a satisfacción de entregable(s) /producto(s) del proyecto, F-GT-9274 Actas de Reunión - No se observan formatos Plan General del proyecto, F-GT-935.Reporte de ejecución y control del proyecto, F-GT-936
	SIGEM Sistema de Gestión Evaluación y Monitoreo	30%	1/05/2022	31/12/2022	- Se evidencian los siguientes Formatos: Solicitud F-GT-192 del 09/05/2022 (Sin número de Ticket). - No se observan los siguientes formatos: Acta de inicio/Constitución del proyecto, F-GT-544. Valoración de complejidad del proyecto, F-GT-930. Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936
Gestión de seguridad y convivencia	App de seguridad	75%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Solicitud F-GT-192 del 14/09/2020 y del 29/10/2021 (Sin número de Ticket). - No se observan los siguientes formatos: Valoración de complejidad del proyecto, F-GT-930. Acta de inicio/Constitución del proyecto, F-GT-544. Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936 Es importante precisar, que pese a que la solicitud del formato F-GT-192 tiene fecha anterior a la vigencia del procedimiento, el inicio del desarrollo tiene fecha posterior a esta por lo tanto aplica la versión 5 del procedimiento objeto de auditoría.

Dependencia o Proceso	Proyecto	Porcentaje de Ejecución I trimestre 2023	FECHA DE INICIO	FECHA DE FINALIZACION	Seguimiento
	PSE - comparendos	30%	1/01/2022	31/12/2022	-No se observan los siguientes formatos: Solicitud F-GT-192 Acta de inicio/Constitución del proyecto, F-GT-544. (Si bien se adjunta documente, este no se encuentra totalmente diligenciado, adicionalmente no cuenta con firmas) Valoración de complejidad del proyecto, F-GT-930. Plan General del proyecto, F-GT-935. (Se adjunta formato sin diligenciar) Reporte de ejecución y control del proyecto, F-GT-936.
Gestión Documental	Buscador de Información	Ejecutado 2022	1/01/2022	30/04/2022	- Se evidencian los siguientes Formatos: Valoración de complejidad del proyecto, F-GT-930. Acta entrega y recibo a satisfacción de entregable(s) /producto(s) del proyecto, F-GT-927 (sin firma del Gerente del proyecto). - No se observan los siguientes formatos: Solicitud F-GT-192 del 14/09/2020 y del 29/10/2021 (Sin número de Ticket). Acta de inicio/Constitución del proyecto, F-GT-544. Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936 Acta de terminación y cierre del proyecto, F-GT-648 No fue posible determinar la fecha de solicitud del proyecto, sin embargo, la fecha de inicio registrada en el PETI corresponde al 1/01/2022.
	SGDA - SIGA	85%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Acta de inicio/Constitución del proyecto, F-GT-544. (Sin firma y sin registro del monto en el presupuesto inicial del proyecto.) - No se observan los siguientes formatos: Solicitud F-GT-192 Valoración de complejidad del proyecto, F-GT-930. Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936

Dependencia o Proceso	Proyecto	Porcentaje de Ejecución I trimestre 2023	FECHA DE INICIO	FECHA DE FINALIZACION	Seguimiento
Gestión Jurídica y Contractual	Hoja de Ruta SICAPITAL - contratación por SISCO	25%	1/01/2022	31/12/2022	-Se evidencian los siguientes Formatos:Solicitud F-GT-192 del 01/02/2021 (Sin número de Ticket).Acta de inicio/Constitución del proyecto, F-GT-544. -No se observan los siguientes formatos: Valoración de complejidad del proyecto, F-GT-930.Plan General del proyecto, F-GT-935.Reporte de ejecución y control del proyecto, F-GT-936 Es importante precisar, que pese a que la solicitud del formato F-GT-192 tiene fecha anterior a la vigencia del procedimiento, el inicio del desarrollo registrado en el PETI tiene fecha posterior a esta, por lo tanto, aplica la versión 5 del procedimiento objeto de auditoría.
	Puesta en funcionamiento solución de apelaciones	92%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Solicitud F-GT-192 del 08/09/2020 (Sin número de Ticket). - No se observan los siguientes formatos: Valoración de complejidad del proyecto, F-GT-930. Acta de inicio/Constitución del proyecto, F-GT-544. Plan General del proyecto, F-GT-935. (Si bien se adjunta formato, este no se encuentra diligenciado) Reporte de ejecución y control del proyecto, F-GT-936 Es importante precisar, que pese a que la solicitud del formato F-GT-192 tiene fecha anterior a la vigencia del procedimiento, el inicio del desarrollo tiene fecha posterior a esta, por lo tanto, aplica la versión 5 del procedimiento objeto de auditoría.
Todos los procesos misionales	Integración de los sistemas de información JUSTICIA- LICO - COPE	60%	1/01/2022	31/12/2022	- Se evidencian los siguientes Formatos: Acta de inicio/Constitución del proyecto, F-GT-544 -No se observan los siguientes formatos: Solicitud F-GT-192 Valoración de complejidad del proyecto, F-GT-930. (Si bien se adjunta documento, No se evidencia la asignación de valores a las diferentes variables, por lo tanto, no se determina la complejidad del proyecto) Plan General del proyecto, F-GT-935. Reporte de ejecución y control del proyecto, F-GT-936

Tabla N°20. Elaboración propia. Fuente Repositorio de información Carpeta PD-GT-04 Gestión de Proyectos de TI

OBSERVACIÓN N° 7: Debilidades en el diseño y ejecución del Procedimiento *"PD-GT-4 Procedimiento Gestión de Proyectos Versión 5":*

Debilidades en la elaboración del procedimiento "PD-GT-4 Procedimiento Gestión de Proyectos Versión 5" respecto a los documentos de registro de salida de las actividades planteadas, ausencia de puntos de control que aseguren la ejecución y cierre del proyecto. Lo anterior, denota falencias en la información y/o documentación a cargo del proceso, como se encuentra señalado en la Guía de "Elaboración y Control de Documentos del Sistema de Gestión".

RECOMENDACIÓN N° 11: Revisar y corregir las debilidades mencionadas en el procedimiento *"PD-GT-4 Procedimiento Gestión de Proyectos Versión 5",* así mismo identificar actividades de control que permitan garantizar el desarrollo secuencial de las actividades según la planificación realizada.

OBSERVACIÓN N° 8: Falencias en la implementación y uso de los formatos mínimos para la Administración y Gestión de Proyectos TI.:

Una vez verificado el repositorio de información compartido por el proceso se evidenció que los 13 proyectos con estado "En Ejecución y Ejecutados" no cuentan con la totalidad de formatos mínimos requeridos para la Administración y Gestión de Proyectos TI, los cuales se mencionan así:

- *Valoración de complejidad del proyecto, F-GT-930.*
- *Acta de inicio/Constitución del proyecto, F-GT-544.*
- *Acta entrega y recibo a satisfacción de entregable(s) /producto(s) del proyecto, F-GT-927 4.*
- *Acta de terminación y cierre del proyecto, F-GT-648.*
- *Plan General del proyecto, F-GT-935.*
- *Reporte de ejecución y control del proyecto, F-GT-936.*

Lo anterior, evidencia falencias en el cumplimiento de lo establecido en el procedimiento *"PD-GT-4 Procedimiento Gestión de Proyectos Versión 5".*

RECOMENDACIÓN N° 12: Priorizar la actualización que se está realizando a los procedimientos, los formatos que se deben utilizar para el desarrollo de las actividades, generando complementariamente los controles que garanticen el uso y aplicación de dichos formatos que en definitiva van a quedar asociados al procedimiento de gestión de proyectos TI en la Secretaría.

OBSERVACIÓN N° 9: Debilidades en el cumplimiento de las fechas establecidas en los Proyectos registrados dentro del Plan Estratégico de Tecnologías de la Información – PETI:

Al realizar verificación el portafolio de proyectos contenido en el numeral 13 del *"Plan Estratégico de Tecnologías de Información PETI*" versión 4 actualizada el 26 de enero de 2023, se observó que la fecha de finalización registrada para 12 proyectos corresponde a 31 de diciembre de 2022, sin embargo, estos registran una ejecución con corte a IV trimestre de 2022 inferior al 100%, lo cual evidencia debilidades en la planeación de la ejecución de los proyectos e incumplimiento de la fecha de finalización establecida en el plan en mención.

RECOMENDACIÓN N° 13: Generar acciones y construir controles que eviten no dar cumplimiento a la planeación de los proyectos establecidos respecto a las fechas determinadas para estos.

3.5.4 PD-GT-6 Procedimiento Gestión de Incidentes o Problemas Versión 5:

Como respuesta a la solicitud inicial de incidentes de seguridad de la información reportados, identificados y gestionados en las vigencias 2022 y 2023, la DTSI, reporta al equipo auditor 13 eventos distribuidos en el periodo comprendido entre el 3 de octubre de 2022 y el 10 de marzo de 2023. El primer tema por mencionar consiste en la inexistencia de un formato oficial dentro del sistema integrado de gestión con el cual se registre y controlen los incidentes de seguridad de la información, para tal situación y como evidencia, fue remitido al equipo auditor el reporte extraído de la herramienta Service Manager con el cual se controla y documenta el tema de eventos de seguridad de la información, a través de servicios con un numero de ticket.

La política de operación número 9 del procedimiento describe las tipologías por las cuales puede ser clasificado un incidente de seguridad de la información que, al contrastarlo con el reporte remitido al equipo auditor, ninguno de los 13 casos tuvo la aplicación de dichas tipologías.

Otro aspecto importante que el equipo auditor resalta consiste en un evento de seguridad de la información presentado y reportado por la dependencia responsable sin recibir el tratamiento de evento tal y como el procedimiento lo estipula, situación que implicó una materialización del riesgo. El detalle de la situación fue reportado en el informe de auditoría especial a Nomina emitido por la Oficina de Control Interno en el mes de junio de 2023.

Aunado a lo anterior, temas como "caídas" o desconexiones de los sistemas de información de la Entidad tampoco se han tramitado como incidentes de seguridad de la información, situaciones que afectan uno de los pilares de seguridad de la información tal como lo es la disponibilidad, cuya definición según ISO 27000 dicta que es la *"propiedad de ser accesibles y utilizables a la demanda por una Entidad autorizada*". A manera de ejemplo se informan los reportes de sistemas como Progressus y SICAS:

Imagen N°04. Fuente: correo electrónico remitido por la DTSI a toda la Entidad el día 30 de mayo de 2023.

Derivado de lo anterior se presentan las siguientes observaciones y oportunidad de mejora:

OBSERVACIÓN N° 10: Falta de alineación y cumplimiento de lo establecido en la política de operación número 9 el procedimiento Gestión de Incidentes o Problemas por el no uso de las tipologías para clasificar y valorar los incidentes de seguridad de la información:
Dentro del reporte de eventos de seguridad de la información remitidos por la DTSI, se observan los campos fechas, ID, descripción, prioridad, impacto, gestión, tratamiento, responsable y estado, sin visualizar la clasificación de los incidentes, de acuerdo con lo definido en la política de operación número 9 del procedimiento gestión de incidentes o problemas el cual describe que "*un incidente de seguridad de la información podrá ser clasificado por la siguiente tabla*:" Ver tabla número 2 Clasificación de incidentes de seguridad, lo anterior, denota falencias en la aplicación de las variables establecidas en el PD.

RECOMENDACIÓN N° 14: Validar y alinear las tipologías contempladas para valorar los incidentes de seguridad de la información dentro de la herramienta de gestión que se tiene definida para tal fin; por otra parte, actualizar la información dentro del procedimiento si el caso lo amerita y finalmente monitorear el uso y aplicación de estas tipologías para cada incidente de seguridad de la información identificado y gestionado en la Entidad.

OBSERVACIÓN N° 11: Debilidades en el registro y tratamiento de incidentes de seguridad de la información, de acuerdo con la política de operación número 7 del procedimiento Gestión de Incidentes o Problemas:
Como resultado de la validación realizada por el equipo auditor, se evidenciaron eventos de seguridad de la información tales como el materializado en el proceso de Gestión de Talento Humano y las caídas o desconexiones de sistemas de información afectando los pilares de disponibilidad e integridad de seguridad de la información, situación que se evidenció en la falta de registro y gestión de los eventos mencionados ocasionando la materialización de riesgos. Lo anterior, incumple lo establecido en la política de operación número 7 del procedimiento Gestión de Incidentes o Problemas.

RECOMENDACIÓN N° 15: Generar una iniciativa por parte de la DTSI que permita fortalecer el tratamiento de los eventos de seguridad de la información que se pueden estar presentando en la Entidad, principalmente en la identificación y catalogación; lo anterior con el fin de minimizar los riesgos por medio de la información recopilada. Para la gestión de los incidentes de seguridad de la información se recomienda basarse en las buenas prácticas de la industria.

OPORTUNIDAD DE MEJORA N° 5: No se tiene contemplado un formato para registro de incidentes de seguridad de la información:
Los incidentes de seguridad de la información se están registrando y asignando por medio de la herramienta Service manager con el cual la DTSI gestiona todos los casos escalados por los usuarios de la Entidad. Dichos casos son asignados al profesional contratista encargado de la seguridad de la información y es de esta manera que se puede extraer el reporte de eventos, ya que dentro de las tipologías del Service manager no se está asignando una como tal asociada a eventos, incidentes o problemas de seguridad, por tanto, es importante validar la pertinencia de usar un formato asociado al procedimiento y formalizado en el sistema integrado de gestión.

RECOMENDACIÓN N° 16: Determinar dentro de la DTSI el diseño e implementación de un formato que permita el registro de eventos de seguridad de la información o tipificar dentro de la herramienta de gestión Service Manager, con el objetivo de poder generar los reportes necesarios, así como

también adjuntar la información soporte o evidencias de cada investigación o validación y en si la cuantificación de dichos eventos.

3.5.5 PD-GT-8 - Administración de Usuarios Versión 4:

Durante el ejercicio auditor se inició con la verificación de los puntos de control asociados al procedimiento en mención:

Punto de control	¿se encuentra redactado como un punto de control? SI/NO	¿Se establece responsable? SI/NO	¿Se establece evidencia? SI/NO	Verificación OCI
-Actividad n° 16 Verificación de la eficacia en la creación de cuentas de aplicativos	NO	NO	NO	Resultado de la verificación se encontró que el procedimiento no especifica el soporte documental que permita evidenciar la aplicación de los controles, adicionalmente, estos se realizan por el mismo profesional que ejecuta la actividad y finalmente no se encuentran redactados en verbo infinitivo.
Actividad n° 24 Verificación de la eficacia en la creación del usuario en directorio activo	NO	NO	NO	

Tabla N°21. Elaboración Propia. Fuente: PD-GT-8 Versión 4 - Administración de Usuarios

Se continuó con la verificación de uso y aplicación de formatos, encontrando lo siguiente:

Actividad	Formato	Validación
Actividad N° 1 Analizar solicitud de administración de usuarios	Solicitud Administración de usuarios- F-GT-285	Se evaluó el reporte enviado por el proceso con la creación de los casos de usuarios "*Reporte casos Formato F-GT-285*", el cual se descarga de la mesa de servicio de la Entidad. En reunión con el proceso aleatoriamente se verificaron los casos de creación de usuario, creación de correo electrónico y usuario de Orfeo. Se identificó que en el Portal MIPG el formato "*Solicitud Administración de usuarios- F-GT-285*" tiene versión 4 del 2020, no obstante, al descargar el formato este es versión 3 del 2019. De acuerdo con la reunión sostenida con los responsables del procedimiento, se encontró desactualización en políticas de operación y puntos de control.

Tabla N°22. Elaboración Propia. Fuente: PD-GT-8 Versión 4 - Administración de Usuarios

3.6 PD-GT-11 Gestión de infraestructura y plataformas tecnológicas Versión 5:

El objetivo del procedimiento gestión de infraestructura y plataformas tecnológicas describe lo siguiente: *"Gestionar componentes de la infraestructura tecnológica de la Secretaría Distrital de Seguridad, Convivencia y Justicia, basados en mejores prácticas de aprovisionamiento, respaldo y restauración, para disponer de los servicios y soluciones tecnológicas que apoyan los procesos misionales y de apoyo de la Entidad".* En el entendido que este procedimiento apunta a todos los componentes de la infraestructura tecnológica de la Entidad, el equipo auditor informa sobre la falta de integración y adición de las actividades de los componentes que se encuentran en operación dentro de las instalaciones del Centro De Comando, Control, Comunicaciones y Cómputo (C4). A manera de ejemplo se menciona que dentro del formato Plan de Backup, F-GT-932, donde se relaciona la información de ejecución de las copias de seguridad de componentes de TI, no se incluyen temas tales como:

- Sistema de Radio.
- Sistema de Video vigilancia.
- Sistemas de información Premier One y VESTA.

OBSERVACIÓN N° 12: Falta de completitud en la información de los componentes de infraestructura tecnológica dentro de las actividades de gestión que se realizan sobre las plataformas tecnológicas de la Secretaría:
El equipo auditor observó que no se tienen incluidos dentro de los planes de backup los componentes o bases de datos de sistemas de información que soportan la operación del C4, tema que debe ser coordinado y gestionado por la DTSI de acuerdo con sus funciones.

Como segundo aspecto, respecto al procedimiento gestión de infraestructura y plataformas tecnológicas, el equipo auditor informa que la política de operación número 9 del procedimiento indica que "*La Dirección de Tecnologías y Sistemas de la Información debe identificar y mantener actualizado el inventario de los activos de infraestructura tecnológica, entendiéndose hardware y software, teniendo relacionados todos los componentes en nube y onpremise".* De acuerdo con esto, dentro del inventario de activos de infraestructura tecnológica suministrado por la DTSI, no se encuentran componentes (items) que se encuentran operando en el Centro De Comando, Control, Comunicaciones y Cómputo (C4), mencionados anteriormente.

De acuerdo con lo informado, no se está contemplando toda la información de la infraestructura de la Entidad, por ende, se incumple el objetivo del procedimiento y las políticas de operación establecidas, generando riesgos de disponibilidad de la información.

RECOMENDACIÓN N° 17: Generar planes de acción e iniciativas por parte de la DTSI para que los componentes tecnológicos que se encuentran operando en el C4 sean incluidos dentro de los planes de backup y demás actividades programadas para cada vigencia. En el mismo sentido, actualizar los inventarios de activos de infraestructura tecnológica contemplando todos los elementos del ámbito tecnológico que se encuentran en el C4 y en general en todos los equipamientos de la Secretaría.

OPORTUNIDAD DE MEJORA N° 6: Uso de formato no controlado- Plan de Mantenimiento Preventivo de Infraestructura Tecnológica (Equipos):
Dentro de la documentación suministrada por la DTSI frente al cumplimiento de las políticas de operación del procedimiento *Gestión de infraestructura y plataformas tecnológicas,* se evidencia el uso del formato plan de mantenimiento, el cual contiene la información de los procesos de mantenimientos contemplados para la infraestructura tecnológica de la Entidad, dentro de los cuales se mencionan los equipos de cómputo (PC), servidores, impresoras, servicios nube, equipos de networking, seguridad perimetral, infraestructura eléctrica y cableado estructurado, frente a esto es importante determinar la pertinencia de la formalización del formato a fin de estandarizar su uso en la ejecución del procedimiento.

RECOMENDACIÓN N° 18: Validar y determinar por parte de la DTSI de la inclusión del formato plan de mantenimiento dentro del sistema integrado de gestión de la Entidad asociado al proceso de gestión de tecnologías de la información.

3.7 PD-GT-12 Control de Acceso a Plataformas Versión 4:

Autenticación de usuarios administradores en firewall:

En sesión de validación con el equipo de la DTSI, frente al tema de control de acceso a plataformas y específicamente la administración del firewall de la Entidad, fue evidenciado por parte del equipo auditor que la opción para doble factor de autenticación por parte de los administradores se encuentra deshabilitada, situación que genera riesgos de confidencialidad e integridad de seguridad de la información.

OPORTUNIDAD DE MEJORA 7: Factor de doble autenticación deshabilitado para los administradores del Firewall de la Entidad:
La oportunidad de mejora se presenta por parte del equipo auditor debido a la debilidad expuesta respecto al doble factor de autenticación el cual se encuentra deshabilitado para el personal que administra el firewall, quien tiene a su vez la función de blindar y proteger la Entidad de intrusiones y ataques entre otras funciones asociadas, por tal motivo, se generan riesgos de seguridad de la información y es por esto que los usuarios administradores deben aplicar los máximos niveles de seguridad posible en su autenticación, principalmente debido a que el soporte se realiza remotamente.

RECOMENDACIÓN N° 19: Verificar que los parámetros de seguridad para autenticación en el Firewall y en general dentro de los componentes de seguridad perimetral cuenten con los máximos niveles y parámetros de seguridad configurados, acompañado de revisiones y monitoreos periódicos por parte del oficial de seguridad de la información de la Entidad.

3.8 PD-GT-17 Ciclo de Vida de Desarrollo de Software Versión 4:

Cronogramas de iniciativas de desarrollo de software gestionados por la DTSI:

Para el procedimiento ciclo de vida de desarrollo de software, el equipo auditor sostuvo sesiones con el equipo responsable, adicionalmente, se realizó validación de la información suministrada por la

DTSI compartida en repositorio de información; basados en esto, en el procedimiento del sistema integrado de gestión se validó la Política de Operación número 2 el cual describe que "*Siempre deberá elaborarse el cronograma de proyecto antes de dar inicio al desarrollo de una aplicación.*". Para tal fin y como se mencionó, el equipo auditor validó la existencia de un tablero de control que opera sobre MS Project donde se lleva el reporte general del estado de las solicitudes o requerimientos con sus respectivos datos generales tales como tiempos y responsables, sin embargo, no fue evidenciado la existencia de los cronogramas estipulados en la política de operación, situación que deriva en el incumplimiento de lo descrito en el SIG de la Secretaría.

OBSERVACIÓN N° 13: No se cuenta con los cronogramas de proyectos estandarizados para todos los requerimientos de desarrollo de software en curso:

La observación de auditoría apunta en primera medida a que no todos los sistemas de información están reportados y publicados dentro del mencionado tablero de control; a manera de ejemplo se identifican sistemas de información de apoyo (SIAP y Sicapital) y misional (SIMBA). Como segundo aspecto, se informa la falta de estandarización y cumplimiento de la política de operación 2 del procedimiento, la cual contempla la generación de los cronogramas para los desarrollos; puntualmente y para ampliar la información de la observación, los siguientes requerimientos validados no tienen cronograma asociado dentro del repositorio compartido por la DTSI:

Sistema de información	Numero de requerimiento o nombre carpeta de ubicación
Argos	1
Progressus	Requerimientos
SIAP	3

Tabla N°23. Elaboración propia. Fuente: Repositorio de información compartido por la DTSI para la auditoria, carpeta PD-GT-15 Gestión de requerimientos tecnológicos

Por lo anterior, se presentan riesgos de incumplimiento del SIG de la Entidad, así como también riesgos por la indisponibilidad de un sistema de información.

RECOMENDACIÓN N° 20: Validar y verificar que todas las iniciativas de desarrollo de software en curso cuenten con sus correspondientes cronogramas y planes de trabajo, así mismo definir una estrategia de control que garantice sobre los desarrollos futuros cumplan lo establecido y descrito dentro del procedimiento. De igual manera definir y estandarizar un formato o documento único de cronograma, con esto, se facilita el monitoreo y revisión del cumplimiento del procedimiento.

Requerimientos funcionales, no funcionales y de seguridad de la información

Derivado de la solicitud de información, el equipo auditor procedió a revisar el cumplimiento de la política de operación número 3 del procedimiento ciclo de vida de desarrollo de software, especialmente donde se menciona que para los desarrollos se deben generar requerimientos de tipo funcional, no funcionales y los de seguridad de la información.

OBSERVACIÓN N° 14: Ausencia de soportes documentales asociados al procedimiento ciclo de vida de desarrollo de software, donde se registran los requerimientos no funcionales y de seguridad de la información de temas tramitados por la DTSI:

Específicamente y al revisar por parte del equipo auditor de manera aleatoria los soportes suministrados por la DTSI, a continuación, se presentan los siguientes casos donde se observa la falta de requerimientos no funcionales y/o de seguridad de la información, incumpliendo lo definido en la política de operación número 3 del procedimiento Ciclo de Vida de Desarrollo de Software así:

Sistema de información	ID/ Caso	Requerimientos Funcionales	Requerimientos no funcionales	Requerimientos de Seguridad de la Información	Comentario OCI
LICO	CU. LICO. SDSCJ. Opciones de certificación 29-06-2022	SI	NO	NO	Tanto en la descripción como en el punto 4 del informe se describe la solicitud, es decir el requerimiento. No se observan dentro del formato requerimientos no funcionales y requerimientos de seguridad de la información.
LICO	20220909 F-GT-646 CU Ajustes recibo de pago LICO	SI	NO	NO	No se observan dentro del formato requerimientos no funcionales y requerimientos de seguridad de la información.
COPE	F-GT-646 Cargue de Asignaciones - COPE v2-1	SI	NO	NO	No se observan dentro del formato requerimientos no funcionales y requerimientos de seguridad de la información.
SIGEM	F-GT-646- 1 CU Gestionar Evaluación Aleatoria	SI	NO	NO	No se observan dentro del formato requerimientos no funcionales y requerimientos de seguridad de la información.

Tabla N° 24. Elaboración propia. Fuente: Evidencias documentales compartidas por la DTSI

Lo anterior genera riesgos por el incumplimiento del procedimiento ciclo de vida de desarrollo de software y específicamente riesgos en los pilares integridad y disponibilidad de la información.

RECOMENDACIÓN N° 21: Establecer una estrategia por parte de la DTSI, que garantice el cumplimiento estricto de lo establecido en el procedimiento. Específicamente definir el documento o formato que van a contener los requerimientos funcionales, no funcionales y de seguridad de la información con su correspondiente lineamiento (pasos o modos) del cómo generar este tipo de solicitudes.

Uso y aplicación de Formatos titulados especificación de requerimientos tecnológicos GT-646 e identificación de necesidad de proyecto GT-192:

Al validar el procedimiento ciclo de vida de desarrollo de software por parte del equipo auditor, se revisaron las actividades 1, 2 y 3, con el fin de establecer el grado del uso de los formatos titulados **especificación de requerimientos tecnológicos** GT-646 e i**dentificación de necesidad de proyecto** GT-192 para cada uno de los requerimientos que se encuentran en trámite. Como resultado se presenta la siguiente observación

OBSERVACIÓN N° 15: No se están generando los Formatos: Especificación de Requerimientos Tecnológicos F-GT-646 e Identificación de Necesidad del proyecto F-GT-192 perteneciente al procedimiento Ciclo de Vida de Desarrollo de Software:

El equipo auditor evidenció que, para requerimientos de sistemas de información tramitados y gestionados por la DTSI, no se está utilizando el Formato Especificación de Requerimientos Tecnológicos F-GT646 el cual debe ser aplicado de acuerdo con las actividades 1, 2 y 3 del procedimiento ciclo de vida de desarrollo de software. Los siguientes son los casos evidenciados:

Sistema de información	Numero de Requerimiento o nombre de carpeta digital
Progressus	Requerimientos
Sidijus	5
Servicios ciudadanos	2
LICO	Actas

Tabla N° 25. Elaboración propia. Fuente: Repositorio de información compartido por la DTSI

También, como se menciona en el título de la presente observación, se observó que para los requerimientos de sistemas de información no se está generando el Formato titulado Identificación de Necesidad del proyecto F-GT192, el cual está definido en la actividad número 1 titulada Gestionar requerimientos tecnológicos del procedimiento. A continuación el detalle del caso evidenciado:

Sistema de información	Numero o nombre de Requerimiento
COPE	Cargue de asignaciones / 2022

Tabla N° 26. Elaboración propia. Fuente: Repositorio de información compartido por la DTSI

RECOMENDACIÓN N° 22: De igual manera a la observación anterior, se recomienda a la DTSI fortalecer las actividades en especial las de control, que permitan el cumplimiento de lo establecido en el procedimiento, generando los formatos asociados a cada actividad descrita y adicionalmente, revisar el modo y método usado para la generación, organización y almacenaje de los soportes derivados de cada requerimiento tramitado al interior de la DTSI.

Uso de formatos no formalizados en el sistema integrado de gestión:

Al revisar la documentación suministrada por la DTSI, el equipo auditor evidenció el uso de formatos sin aprobar en el sistema integrado de gestión

OPORTUNIDAD DE MEJORA N° 8: Uso de formatos en el procedimiento ciclo de vida de desarrollo sin formalizar en el Sistema integrado de gestión de la Entidad:
Dentro de la revisión a la documentación asociada al cumplimiento del procedimiento, se **evidenció** el siguiente caso:

Para el sistema de información Progressus el uso del formato nombrado 20210920-CC_ACTUALIZACIÓN-VALORES-ESTRATEGIAS

Imagen 05. Formato 20210920-CC_ACTUALIZACIÓN-VALORES-ESTRATEGIAS

De acuerdo con lo expresado anteriormente la oportunidad de mejora se presenta por el uso de formatos no controlados, los cuales no están formalizados en el sistema integrado de gestión - portal MIPG, generando riesgos de incumplimiento lo allí estipulado.

RECOMENDACIÓN N° 23 Realizar por parte de la DTSI una revisión de los soportes documentales asociados a cada uno de los requerimientos que se encuentran en curso, garantizando que se utilicen los formatos oficiales del procedimiento. Complementariamente reforzar con el personal encargado, el uso y aplicación de los formatos oficiales del procedimiento.

Planes de trabajo para los requerimientos de desarrollo estimados en el procedimiento ciclo de vida de desarrollo de software:

A continuación, se presentan los casos evidenciados por el equipo auditor frente a la falta del acta o soporte que demuestra la *generación del plan de trabajo con actividades granulares* tal y como lo estipula la actividad 3 del procedimiento Ciclo de Vida de Desarrollo de Software, la cual describe "*Estimar el esfuerzo necesario para realizar el desarrollo, actualizando en el cronograma los tiempos de implementación de los requerimientos y actividades.*":

- **Servicios Ciudadanos Requerimiento 01:** No se visualiza el acta de reunión resultante con el plan de trabajo estimado del ciclo de desarrollo de software tal como lo determina la actividad 3 del procedimiento. Únicamente se visualizan dos actas de seguimiento y el formato código 647

- COPE 2022: Los soportes del requerimiento tramitado en 2022 para COPE, no evidencian el plan de trabajo estimado en un acta de reunión. Dentro de los soportes remitidos, se visualizan un acta de seguimiento y el formato código 646 sobre cargue automático de asignaciones.
- SIMBA requerimiento 02: Se evidencian actas de aprobación plan de trabajo y estado actual de Simba en el módulo de combustible, sin embargo, no se observa acta con el plan de trabajo propiamente. Se menciona un acta con el estado actual, conteniendo compromisos y se presenta lo que se va a realizar, pero no se reportan fechas y responsables.
- SIDIJUS: Para los 6 requerimientos revisados, en ninguno de los casos se observa acta con el plan de trabajo.

OBSERVACIÓN N° 16: Debilidades en el cumplimiento de la Actividad 3 del procedimiento Ciclo de Vida de Desarrollo de Software respecto a la generación del Plan de trabajo con actividades granulares:
De acuerdo con los casos presentados en el párrafo anterior, no se ha generado el plan de trabajo para los requerimientos de desarrollo, por tanto, la observación de auditoría se informa por la falta puntual de los soportes definidos en la actividad 3 del procedimiento ciclo de vida de desarrollo de software, en el que se requiere generar un plan de trabajo con el detalle de las actividades granulares, situación que redunda en riesgos que afectan la planeación y ejecución de actividades estimadas para cada desarrollo.

RECOMENDACIÓN N° 24: Definir acciones por parte de los responsables de ejecutar el procedimiento Ciclo de vida de desarrollo de software en la DTSI para que refuercen la ejecución de la actividad número 3 respecto a cada uno de los requerimientos de desarrollo que sean escalados y tramitados, así como también definir el documento, formato, estándar o acta que refleje el plan de trabajo. Complementariamente estimar la necesidad de modificar o actualizar dentro del procedimiento la actividad puntualizando el entregable que debe emitirse por los responsables.

Documento de aseguramiento de calidad del dato contemplado en el procedimiento ciclo de vida de desarrollo de software.

Realizando revisión del procedimiento y específicamente en la actividad número 7 del procedimiento, una de las salidas que se debe generar es el "*Documento en Excel de aseguramiento de la calidad del dato actualizado cuando aplique*". Durante el ejercicio auditor se evidenció la falta de generación de dicho soporte en las vigencias 2022 y 2023, configurando la siguiente observación de auditoría:

OBSERVACIÓN N° 17: Falta de Documento que refleje el Aseguramiento de calidad del dato de acuerdo con la actividad número 7 del procedimiento Ciclo de Vida de Desarrollo de Software:
No se observó la emisión o generación del documento que asegure la calidad de dato para los requerimientos tramitados en las vigencias 2022 y 2023, de acuerdo con la revisión realizada a los soportes documentales presentados por la DTSI. Adicionalmente, se informa que este soporte está contemplado como una salida de la actividad 7 en el procedimiento, pero no se ha formalizado en el SIG de la Entidad.

RECOMENDACIÓN N° 25: Estimar y ejecutar actividades conjuntas dentro de la DTSI, para que se genere el documento **aseguramiento de calidad de dato** mencionado dentro del procedimiento ciclo

de vida de desarrollo del software, ya que éste cumple con una función importante consistente en la validación de los datos durante todo el ciclo de desarrollo de un requerimiento.

Uso del formato requerimientos tecnológicos:

OBSERVACION 18: No se está usando el formato de pruebas a requerimientos tecnológicos F-GT-647 para casos de desarrollo de software en la DTSI basado en la actividad número 9 del procedimiento ciclo de vida de desarrollo de software:
Al validar el uso del formato pruebas a requerimientos tecnológicos F-GT-647 correspondiente a la actividad número 9 del procedimiento Ciclo de Vida de Desarrollo de Software, se realiza revisión aleatoria de requerimientos a diferentes sistemas de información, reportando que los siguientes casos no se les ha creado o diligenciado el mencionado formato:

- SIAP requerimiento 006.
- SIGEM requerimiento 001.
- Progressus (Ningún requerimiento).
- SIMBA (Ninguno de los 5 requerimientos)

Lo anterior, denota incumplimiento frente al procedimiento establecido, ocasionando riesgos de integridad y fallas en la funcionalidad de los sistemas de información.

RECOMENDACIÓN N° 26: Determinar las acciones y controles necesarios que garanticen la aplicación y uso del formato para requerimientos futuros.

Uso de los formatos gestión de cambios y bitácora de actividades en la ejecución de las actividades asociadas al procedimiento:

OBSERVACIÓN 19: Falta de cumplimiento de la Actividad 12 del procedimiento ciclo de vida de desarrollo de software por la ausencia de los formatos F-GT-277 y F-GT-278:
La actividad número 12 del procedimiento ciclo de vida de desarrollo de software describe la elaboración del requerimiento de cambios RFC, el cual presenta como salida el formato gestión de cambios de TIC F-GT-278 y el Formato Bitácora de actividades F-GT-277; al validar los soportes remitidos por la DTSI frente a estos dos formatos, se observan 18 formatos de requerimientos de cada uno de los mencionados, no obstante, la observación se presenta debido a que no se han generado los formatos para todos los requerimientos entre los cuales se mencionan:

Sistema de información	Actividad o Descripción	Estado del requerimiento	Fecha de entrega
ARGOS	Realizar una funcionalidad de cargue masivo	Completa	12/05/2023
SIMBA	Módulo Comodatos: Actividades Iniciales: Análisis de Requerimientos; Taller de Entendimiento; Documento funcional de la Solución; Definición de la Plataforma; Arquitectura de Integración hardware; Diseño Arquitectura de Solución.	Completa	27/02/2023

Sistema de información	Actividad o Descripción	Estado del requerimiento	Fecha de entrega
PROGRESSUS	Implementar una funcionalidad para poder "abrir" y "cerrar" la posibilidad de cargar avances, y también la posibilidad de "abrir y cerrar" periodos ya cumplidos, para que la información previamente cargada y validada no tenga modificaciones posteriores sin previa aprobación del rol "director".	Completa	No registra en listado de requerimientos

Tabla N° 27. Elaboración propia. Fuente: Repositorio de información compartido por la DTSI para la auditoria, carpeta PD-GT-02 Procedimiento Gestión de Cambios de TIC

En otra medida, se evidenciaron formatos F-GT-278 que apuntan a sistemas de información sin estar registrados o catalogados dentro del inventario vigente de requerimientos de la DTSI así:

Sistema de información	Ticket	Fecha
Portal MIPG	SR196520	19/01/2023
SISIPEC	SR201607	23/02/2023
LICO	SR203345	08/03/2023

Tabla N° 28. Elaboración propia. Fuente: Repositorio de información compartido por la DTSI para la auditoria, carpeta PD-GT-15 Gestión de requerimientos tecnológicos

De acuerdo con lo anterior, se presentan riesgos de incumplimientos frente a la documentación establecida en el Sistema Integrado de Gestión de la Entidad, así como también omisiones en la ejecución de las actividades por parte del personal responsable.

RECOMENDACIÓN N° 27: Determinar las acciones necesarias que garanticen la aplicación y uso del formato para requerimientos futuros, con sus correspondientes excepciones.

3.9 PD-GT-18 Procedimiento Gestión de Datos Abiertos Versión 1:

Una vez revisada la estructura del procedimiento *"Gestión de Datos Abiertos - PD-GT-18-V-1"* se pudo determinar que:

El objetivo y el alcance del procedimiento abordan de manera adecuada los aspectos fundamentales de la gestión de datos abiertos y establecen un marco claro para el procedimiento.

- Las políticas de operación abarcan diferentes aspectos relevantes para la gestión de datos abiertos en la Secretaría Distrital de Seguridad, Convivencia y Justicia, tales como responsabilidades claras, promueven la calidad de los datos, se encuentran encaminadas a garantizar la disponibilidad y reutilización de estos, y fomentar la planificación y evaluación continua.

- Punto de control en la actividad 7: *"Verificar la divulgación de datos abiertos en los canales internos y externos de la Entidad*". Este punto de control tiene como objetivo asegurarse de que los conjuntos de datos abiertos sean debidamente comunicados tanto dentro de la

Entidad (canales internos) como fuera de ella (canales externos). Sin embargo, el registro de salida no permite identificar la trazabilidad del punto de control registrado.

- Las actividades descritas en el procedimiento, no se encuentran alineadas al Plan de Apertura de datos Abiertos, las actividades y registros asociados no involucran los formatos F-GT-913, F-GT-914, F-GT-915.

Validación del Procedimiento:

Para la validación del procedimiento se verificó la implementación de las políticas de operación del procedimiento, así como de las actividades descritas en este, encontrando:

- El Plan de Apertura de Datos fue documentado por el proceso de Gestión de la Tecnología de Información mediante archivo PL-GT-5 el cual a la fecha se encuentra en versión 1, en este se identifica el ecosistema de actores, se establecen los roles, se mencionan los sistemas de información de la Entidad, portales web y App, con un total de 26 conjuntos de datos abiertos los cuales se relacionan a continuación:

ítem	Conjunto de datos Abierto	Dependencia que genera el Conjunto de Datos Abierto	Frecuencia de
1	Delito de Alto Impacto. Bogotá D.C.	Oficina de Análisis de Información y Estudios	Mensual
2	Incidente Reportado. Centro de Comando, Control, Comunicaciones y Cómputo de Bogotá - C4 Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Mensual
3	Medida Correctiva. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Mensual
4	Incidentes Tramitados en el C4 - Numero Único de Seguridad y Emergencias NUSE. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Mensual
5	Comando de Atención Inmediata. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
6	Cuadrantes de Policía. Bogotá D.C	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
7	Estación de Policía. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
8	Comando Operativo de Seguridad Ciudadana. Bogotá D.C	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
9	Inspección de Policía. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
10	Cárcel. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral

ítem	Conjunto de datos Abierto	Dependencia que genera el Coniunto de Datos Abierto	Frecuencia de
11	Unidad de Reacción Inmediata. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
12	Centro de Traslado por Protección. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
13	Sistema de Responsabilidad Penal para Adolescentes. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
14	Casa de Justicia. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
15	Centro de Convivencia. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
16	Unidad de Mediación y Conciliación. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
17	Centro de Atención a Víctimas Delito Sexual y Violencia IntraFamiliar. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
18	Punto de Atención Comunitaria. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
19	Consejo de Justicia. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
20	Unidad de Rama Judicial. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
21	Unidad de Fiscalía. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
22	Sala de Atención al Usuario. Bogotá D.C.	Oficina de Análisis de Información y Estudios Estratégicos	Semestral
23	Centro de Comando, Control, Comunicaciones y Cómputo de Bogotá - C4 Bogotá D.C.	Oficina de Análisis de Información y Estudios	Semestral
24	Índice de Información Clasificada y Reservada SSCJ Bogotá D.C.	Dirección de Recursos Físicos y Gestión Documental	Anual
25	Registro de activos de información de la SD-SCJ Bogotá D.C.	Dirección de Recursos Físicos y Gestión Documental	Anual
26	Esquema de Publicación SDSCJ. Bogotá D.C.	Oficina Asesora de Planeación	Anual

Tabla N°29. Conjunto de Datos Abiertos SDSCJ - Fuente: Plan de Datos Abiertos PL-GT-5 Versión 1"

Teniendo en cuenta la información de la tabla anterior, se procedió a verificar la publicación de los conjuntos de datos abiertos en la página datosabiertos.bogota.gov.co encontrando que en esta se registra un total de 19 conjuntos, lo cual difiere de lo registrado en el Plan de Apertura de datos y en

lo publicado en la página web de la Entidad, a continuación, se relacionan los 7 conjuntos de datos que no se encuentran publicados en el portal en mención:

Imagen N°06. Conjunto de Datos Abiertos SDSCJ - Fuente: Plan de Datos Abiertos PL-GT-5 Versión 1" - https://datosabiertos.bogota.gov.co/organization/secretaria-distrital-de-seguridad-convivencia-y-justicia

- Por otra parte, las políticas de operación establecen que la identificación de los conjuntos de datos abiertos susceptibles de publicación se realiza bajo lo establecido en el Formato *"Matriz para la identificación y Caracterización de los Archivos de Información para el Plan de Apertura, Mejora y Uso de Datos F-GT-915"*, así las cosas, el formato remitido por el proceso objeto de auditoria cuenta con 51 registros, sin embargo, al verificar la columna "*Vinculo a Datos Abiertos (Si aplica)*" ninguno de estos cuenta con un vínculo registrado por lo cual no fue posible identificar la caracterización de los archivos de información correspondiente a los conjuntos de datos en el formato en mención.

- En lo correspondiente a la priorización y programación, esta se debe realizar en el formato *"Matriz Plan de Apertura, Mejora y Uso de Datos F-GT-914" al* verificar este, se observó que cuenta con el registro de 24 conjuntos de datos, no se evidencia el registro de los conjuntos de datos Esquema de Publicación SDSCJ. Bogotá D.C. e Inspección de Policía Bogotá D.C., adicionalmente, la variable "Fecha de implementación" solo contiene datos para Registro de Activos de Información - Índice de Información Clasificada y Reservada.

- Es importante precisar que los formatos F-GT-914 y F-GT-915 no cuentan con un espacio para el registro de la fecha en la cual se actualiza el contenido de la información registrada, por lo tanto, no es posible determinar en qué fecha se realizó el diligenciamiento de esta.

- De acuerdo con lo establecido en el "*Plan de Apertura de datos Abiertos PL-GT-5"* Versión 1 se evidencio el Formato *"Documentación de Datos Abiertos F-GT-913" los* conjuntos de datos Índice de Información Clasificada y Reservada SSCJ Bogotá D.C., Registro de activos de información de la SD-SCJ Bogotá D.C., Esquema de Publicación SDSCJ. Bogotá D.C. e Inspección de Policía Bogotá D.C. no cuenta con el formato en mención.

- Por último, no se allego por parte del proceso auditado la actualización del documento "*Plan de Apertura de datos Abiertos PL-GT-5" teniendo* en cuenta la actividad número 7 programada en el documento en mención para el 31 de marzo de 2023.

OBSERVACIÓN N° 20: Debilidades en la Elaboración del Procedimiento *"Gestión de Datos Abiertos - PD-GT-18-V-1":*

Debilidades en la elaboración del procedimiento *"Gestión de Datos Abiertos - PD-GT-18-V-1" respecto* registro de salida del punto de control establecido en la actividad N°7, alineación con el Plan de Apertura de datos Abiertos, lo cual implica la relación de los formatos F-GT-913, F-GT-914 y F-GT-915 en el registro de ejecución de las actividades. Lo anterior, denota falencias en la información y/o documentación a cargo del proceso, como se encuentra señalado en la Guía de "*Elaboración y Control de Documentos del Sistema de Gestión".*

RECOMENDACIÓN N° 28: Revisar y corregir las debilidades identificadas en el procedimiento *"Gestión de Datos Abiertos - PD-GT-18-V-1"*. Como actividad complementaria, se sugiere dejar trazabilidad en el registro de salida del punto de control y asegurar que las actividades se encuentren alineadas con lo establecido en el Plan de Apertura de datos Abiertos de la Entidad.

OBSERVACIÓN N° 21: Falencias en la implementación del Plan de Apertura de datos Abiertos:

Una vez verificado el Plan de Apertura de datos Abiertos, se identificó que 7 conjuntos de datos abiertos de la SDSCJ no se encuentran publicados en la plataforma del Distrito, se presentan debilidades en la implementación y uso de los formatos F-GT-913, F-GT-914 y F-GT-915, así mismo, no se allegó soporte de actualización del plan en mención para la vigencia 2023, lo anterior, evidencia falencias en lo establecido en el Plan de Apertura de datos Abiertos PL-GT-5 V-1.

RECOMENDACIÓN N° 29: Llevar a cabo una revisión exhaustiva y una actualización de los procedimientos, políticas y formatos utilizados para el tema de datos abiertos. Así mismo, se sugiere alinear las actividades y registros del procedimiento con el Plan de Apertura de Datos Abiertos, asegurando que los conjuntos de datos sean debidamente caracterizados, priorizados y programados. Además, es importante establecer mecanismos claros y efectivos para la divulgación de los conjuntos de datos tanto internamente como externamente, asegurando la trazabilidad de esta actividad. Por último, se recomienda realizar la actualización del "Plan de Apertura de Datos Abiertos PL-GT-5" y garantizar que todos los conjuntos de datos sean debidamente publicados en el portal de datos abiertos correspondiente. Estas acciones contribuirán a fortalecer la gestión de datos abiertos, promover la transparencia y garantizar el cumplimiento de la normatividad vigente.

3.10 Política y Manual de privacidad y seguridad de la información de la Entidad Versión 3:

Valoraciones de seguridad de la información en proyectos de TI:

Se solicita en mesa de trabajo con la DTSI evidencias que reflejen las valoraciones de seguridad de la información en los proyectos de TI que se encuentran en curso, a lo cual fue remitido a esta Oficina diferentes soportes como actas, formatos, reportes e informes donde seguridad de la información (Oficial de Seguridad) ha participado en proyectos generando comentarios, específicamente a SIGA y APP de seguridad de Cárcel Distrital.

OBSERVACIÓN N° 22: No se evidencia la valoración de seguridad de la información en la administración y gestión de proyectos de la Entidad de acuerdo con lo estipulado en el numeral 5.2.5 del manual de seguridad y privacidad de la información con relación a la gestión de proyectos:
La observación de auditoría apunta a la falta ejecución de la valoración de seguridad definida en el manual de seguridad y privacidad de la información para todos los proyectos a nivel de TI que se encuentran en curso y reportados en el PETI vigente, dentro de los cuales se mencionan:

- Registro Sistemas de Video vigilancia (acuerdo 816).
- Hoja de Ruta SICAPITAL - contratación por SISCO.
- SIMBA Fase II.
- Integración de los sistemas de información JUSTICIA- LICO – COPE.
- Buscador de Información.
- Puesta en funcionamiento solución de apelaciones.
- SIGEM Sistema de Gestión Evaluación y Monitoreo.

Lo anterior, incumple lo establecido en el numeral 5.2.5 titulado **seguridad de la información en la gestión de proyectos** dentro del manual de seguridad y privacidad de la información Versión 3 de la Entidad, adicionalmente, nos permitimos informar riesgos de seguridad de la información por las debilidades que se pueden generar en cada desarrollo o mejora de software al no contar con el diagnóstico y la perspectiva de seguridad de la información.

RECOMENDACIÓN N° 30: Establecer por la DTSI acciones encaminadas a fortalecer la ejecución de esta actividad por medio de la emisión de conceptos por parte del Oficial de Seguridad de la Información, la cual es de carácter importante para todos los proyectos que se realicen en la Entidad en materia de Tecnologías de la Información, lo anterior acompañado de un proceso de monitoreo y revisión que garantice el cumplimiento cabal tal como lo establece el manual de seguridad y privacidad de la información.

Diligenciamiento del formato compromiso de confidencialidad y no divulgación de la información:

De acuerdo con el numeral 5.3.2. del Manual de Seguridad y Privacidad de la información el cual define que ," *Los funcionarios o contratistas vinculados a la Entidad, deben acatar y cumplir lo requerido en la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", Ley 1712 de 2014 "Ley de Transparencia y acceso a la Información Pública" así como lo exigido en la PO-GT-01 "Política de Seguridad y Privacidad de la Información", MA-GT-01 "Manual De Seguridad y Privacidad de La Información" de la Entidad. Por otra parte, deben diligenciar el formato F-GH-807 "Compromiso de Confidencialidad y no Divulgación de la Información" al inició del empleo y demás normatividad relacionada con seguridad de la información aplicable a la Entidad.*"
Complementariamente se mencionan los numerales 5.5.6 Gestión de información secreta para la autenticación de usuarios, 5.9.4 Políticas y Procedimientos de Transferencia de Información y 5.9.7 Acuerdos de Confidencialidad o de no Divulgación. De acuerdo con estos lineamientos, se valida con la DTSI el cumplimiento, evidenciando que para el personal de planta se realiza generando el formato y adjuntándolo al expediente que reposa en la Dirección de Talento Humano, pero para el personal contratista no se está generando, derivando en la siguiente observación.

OBSERVACIÓN N° 23: Debilidades en la aplicación de lo establecido en el numeral 5.3.2 con título Término y condiciones del empleo del Manual de Seguridad y Privacidad de la información versión 3 de la Entidad asociado a la falta de diligenciamiento del formato F-GH-807 "Compromiso de Confidencialidad y no Divulgación de la Información" por parte del personal contratista de la Entidad:
No se está generando ni diligenciado el formato F-GH-807 "Compromiso de Confidencialidad y no Divulgación de la Información para el personal contratista de acuerdo con lo estipulado en el numeral 5.3.2 con título Término y condiciones del empleo del Manual de Seguridad y Privacidad de la información versión 3 de la Entidad, sumado a que no existe coherencia con el título establecido vs lo señalado en el desarrollo de este, frente a la aplicación del formato mencionado. De acuerdo con lo informado, esta Oficina indica la existencia de riesgos reputacionales y de confidencialidad de la información tales como fuga de información, por el no cumplimiento de lo definido en el manual.

RECOMENDACIÓN N° 31: Generar planes de acción conjuntos con las dependencias responsables para garantizar que el formato sea diligenciado por todo el personal de planta y los contratistas tal y como lo estipula el manual de seguridad y privacidad de la información de la Entidad. Complementariamente, determinar el repositorio ya sea físico o virtual donde se vayan a almacenar los formatos de contratistas. Finalmente se recomienda actualizar los datos y lineamientos consignados en el manual de seguridad y privacidad de la información.

Inactivación de usuarios en los sistemas de información de la Entidad:

El equipo auditor realiza validación de las actividades ejecutadas respecto a la inactivación de usuarios en los sistemas de información de la Entidad. En primera medida se valida que para los contratistas al momento de finalizar el vínculo contractual se inicia un proceso escalonado donde participan las diferentes dependencias de la Entidad firmando un paz y salvo cuya culminación se da al momento de la inactivación de los usuarios en los sistemas de información, cabe resaltar que al momento de inactivar el usuario en el directorio activo automáticamente se replican a los sistemas de información conectados. Para el personal de planta, mensualmente la Dirección de Talento Humano remite a la DTSI el reporte con las novedades de personal tales como ausencias, incapacidades, vacaciones, entre otras, para que por medio de un ticket de servicio sean aplicados estos cambios sobre los sistemas de información.

OBSERVACIÓN N° 24: Falta de ejecución completa de la actividad que inactive los usuarios matriculados en los sistemas de información de la Entidad:
El numeral 5.3.6 del manual de seguridad y privacidad de la información titula terminación o cambio de responsabilidades de empleo y específicamente el literal a) describe "La Dirección de Gestión Humana se encarga de notificar a través de los medios autorizados para tal fin (Correo electrónico institucional o herramienta de gestión, o ticket mesa de servicio), a la Dirección de Tecnologías y Sistemas de la Información, todas las novedades de los funcionarios como vacaciones, incapacidades médicas, suspensiones, términos laborales, para que se bloquee o suspendan los privilegios de acceso a las diferentes soluciones tecnológicas de la Entidad, según sea el caso".

De acuerdo con lo anterior, se reitera la observación presentada por esta oficina en el informe de la auditoría especial a nómina la cual titula **Usuarios retirados, con contrato finalizado o que no pertenecen a las dependencias relacionadas con nómina que continúan activos en el sistema SIAP:**

USUARIO_BD	NOMBRE_OPERADOR
ACAMARGO	ALBERTO DE JESUS CAMARGO PARDO
JGUTIERREZ	JUAN AGUSTIN GUTIERREZ GUAQUETA
JDIAZ	JOSE LUIS DIAZ FONTALVO
FMANCERA	FREDY ALEXANDER MANCERA TOLOSA

Tabla N° 30. Elaboración Propia: Fuente Informe auditoria especial de nómina año 2023

Con lo expuesto, las actividades de control que se desarrollan para la inactivación de usuarios en los sistemas de información de la Entidad no se están ejecutando al 100%, ya que están quedando usuarios activos, generando riesgos de confidencialidad e integridad de la información.

RECOMENDACIÓN N° 32: Validar por parte DTSI el funcionamiento de todas las acciones realizadas tanto desde el reporte que realiza la Dirección de Gestión Humana en referencia al personal de planta como la Dirección Jurídica para los contratistas, hasta el cierre del caso (ticket) para que la inactivación de los usuarios se aplique y sea efectiva sobre todos los sistemas de información de la Entidad. Complementariamente se recomienda validar cómo están funcionando estos controles en el C4 para los sistemas de información donde ingresan personal de planta, contratistas y operadores.

Matricula o creación de usuarios en los sistemas de información:

Actualmente para el registro de usuarios en los sistemas de información de la Entidad se siguen los lineamientos estipulados en el procedimiento administración de usuarios PD-GT-8, el cual consiste en el diligenciamiento del formato Solicitud Administración de Usuarios F-GT-285. Este formato es generado por los líderes de cada dependencia o supervisores solicitando los accesos a los sistemas de información y remitiéndolos directamente a la DTSI para su respectivo trámite.

OBSERVACIÓN N°25: Falta de autorización de líder funcional para matricular usuarios en los sistemas de información de la Entidad:

De acuerdo con lo expresado la observación se presenta debido a que no se está recibiendo autorización por parte de los líderes del proceso o dueños de la información para que los diferentes usuarios accedan a los sistemas, es decir está pasando directamente desde la dependencia solicitante hasta la DTSI.

Por otra parte, cuando un contratista se retira de la Entidad y como se mencionó anteriormente, se tramita la paz y salvo con el cual la DTSI bloquea los accesos a los sistemas de información principalmente por el directorio activo. Como es de conocimiento, sistemas de información de la Entidad no validan, identifican y autentican usuarios por medio del directorio activo como es el caso de SICAPITAL, por ende, su inactivación tiene que realizarse directamente sobre el sistema de información y es allí donde se están quedando usuarios en estado activo con contrato finalizado situación reportada en el informe de auditoría especial a nómina.

De acuerdo con estos dos temas presentados, se presenta incumplimiento del numeral 5.5.3 titulado "*registro y cancelación del registro de usuarios"* perteneciente al manual de seguridad y privacidad de la información versión 3 de la Entidad y derivando en riesgos de accesos no autorizados a los sistemas de información, impactando los pilares de integridad y confidencialidad de la información.

RECOMENDACIÓN N° 33: Ejecutar por parte de la DTSI una revisión minuciosa de lo establecido en el manual de seguridad y privacidad de la información y dentro de los procedimientos frente al método utilizado para creación y autorización de cuentas de usuario en los sistemas de información, enfatizando y de acuerdo con las buenas prácticas de seguridad de la información que los accesos deben ser siempre aprobados y autorizados por los dueños de la información o líderes funcionales.

Aplicación de políticas de seguridad para autenticación de usuarios en el directorio activo:

Se realiza prueba con la cuenta del auditor líder cambiando la contraseña en la sesión de Windows para el Directorio Activo y al configurar una clave que tiene parte del nombre de usuario (4 caracteres alfabéticos), ha sido aceptada por el sistema. Lo anterior genera la siguiente observación.

OBSERVACIÓN N° 26: Debilidad en la aplicación de reglas y parámetros para las contraseñas del directorio activo de la Entidad:

La situación expuesta anteriormente implica incumplimiento del literal b del numeral 5.5.12 titulado "*sistema de gestión de contraseñas"* del manual de políticas de seguridad y privacidad de la información, el cual describe que *"No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos."*

Complementariamente, el literal a define el tiempo de caducidad de las contraseñas a 45 días para el acceso a equipos de cómputo, sin mencionar una regla o parámetro para los sistemas de información de la Entidad.

Los aspectos presentados generan riesgos de confidencialidad e integridad de datos, debido a las debilidades de las reglas actualmente configuradas y parametrizadas para las contraseñas, principalmente del directorio activo.

RECOMENDACIÓN N° 34: Realizar una revisión por parte de la DTSI de los parámetros y las reglas de contraseñas utilizadas y aplicadas en directorio activo, sistemas de información y bases de datos de la Entidad para que estas sean homogéneas, fuertes y se alineen a la política de seguridad de la información de la Entidad y con las buenas prácticas de la industria.

Inventario de programas utilitarios que se utilizan en la Entidad:

Se solicita a la DTSI reporte o inventario de programas utilitarios usados dentro de la Entidad, para lo cual fue remitido como soporte un listado de 23 ítems de software base y otros instaladores.

OBSERVACIÓN N° 27: Falta de completitud y formalización del Registro del uso de programas utilitarios en la Entidad:

Después de validar la información suministrada por la DTSI, la observación de auditoría se presenta debido al no cumplimiento de lo establecido en el numeral 5.5.13 titulado "Uso de programa utilitarios privilegiados" del manual de seguridad y privacidad de la información versión 3 de la Entidad, específicamente en el literal E que describe sobre el registro del uso de programas utilitarios del sistema dentro de la Entidad. Este registro no se había construido en la primera sesión de auditoría donde se habló del tema, no obstante, la DTSI remitió un archivo con un inventario de software el cual no contiene todos los ítems de software. Dentro de los programas utilitarios conocidos por el grupo auditor y que son usados dentro de la Secretaría se mencionan:

- Survey 123.
- EPass2003.
- Enterprise Arc.
- Nmap.
- Rstudio.
- TeXstudio.

Complementario a lo anterior, el soporte donde se entrega la información de programas utilitarios en la Entidad, no se encuentra dentro de un formato oficial perteneciente al sistema integrado de gestión. Lo anterior genera riesgos por el hecho de no tener identificados ni catalogados software que soporte la ejecución de las actividades por parte de las dependencias de la Entidad.

RECOMENDACIÓN N° 35: Contemplar y analizar la construcción de un documento formal por parte de la DTSI dentro del sistema integrado de gestión el cual contenga el reporte de software y programas utilitarios usados en todas las dependencias de la Entidad, garantizado su continua actualización.

Controles de acceso físico a equipamientos de TI:

Se realiza visita por parte del equipo auditor en conjunto con la DTSI a los pisos 6, 13 y 14 de la Secretaría, con el fin de validar la operación de los controles de acceso físico, especialmente al centro de cómputo, centros de cableado y en general observando la conexión física de los equipos de cómputo a las fuentes de poder (canaletas).

OBSERVACIÓN N°28: Falta de cumplimiento de los controles establecidos para el ingreso a los centros de cableado:

El equipo auditor al ingresar a los centros de cableado de los pisos 6,13 y 14 en compañía del personal de soporte de la DTSI asignado para la ejecución de la prueba, observó el no cumplimiento de lo establecido en el tercer párrafo del numeral 5.7.2 del manual de seguridad y privacidad de la información, el cual describe que "El ingreso a los centros de cableado en las diferentes áreas será con el aval de la Dirección de Recursos Físicos y Gestión Documental, para lo cual, la Dirección de Tecnologías y Sistemas de la Información o la persona que se delegue mediante correo electrónico, solicitará la autorización de ingreso de usuarios permanente y/o temporal a dichos cuartos para actividades de soporte tecnológico que se requiera, el ingreso debe estar registrado mediante una bitácora con la siguiente información: a. Nombre completo de quien realiza el ingreso. b. Fecha de ingreso. c. Actividad a realizar. d. Tipo y número de documento. e. Administradora de Riesgos Laborales. f. Nombre de la empresa (si aplica). g. Nombre de la persona que hará el acompañamiento", lo mencionado debido a que, durante la visita realizada, no se diligenció ningún tipo de bitácora y también este aspecto se refuerza debido a que en la semana del 12 al 16 de junio se presentó ingreso de personal de mantenimiento al centro de cableado del piso 6 sin evidenciar la bitácora registrando su acceso. Lo anterior genera riesgos de disponibilidad por acceso de personal no autorizado y/o monitoreado.

RECOMENDACIÓN N° 36: Ejecutar un proceso de revisión conjunta entre la DTSI con la Dirección de Recursos Físicos y Gestión Documental de lo contemplado en el manual de seguridad y privacidad de la información versus las acciones y los controles actualmente implementados para actualizar la información y evitar las diferencias evidenciadas.

OBSERVACIÓN N° 29: Situaciones de conexión física de equipos de cómputo evidenciadas en la revisión del cableado estructurado de acuerdo con política de seguridad de información:

Como se mencionó en el punto anterior, se realizó recorrido por los pisos 6, 13 y 14 con el fin de validar el estado y modo de conexión de los equipos de cómputo asignados a los funcionados, del cual se presentan las siguientes situaciones:

Piso	Numero de puesto de trabajo	Observación
14	150	Se tiene conectada a la corriente regulada una multitoma, esta a su vez contiene varios equipos tales como cargadores de radio transistor y celular.
14	171c	El equipo de cómputo se encuentra conectado a la corriente normal (toma blanca).
14	164	Se observan varios recipientes con líquidos cerca a la toma de corriente normal.
14	107	El equipo de cómputo se encuentra conectado a la corriente normal (toma blanca).
13	272	El equipo de cómputo se encuentra conectado a la corriente normal (toma blanca).
13	175.B	La canaleta se encuentra abierta con el cableado expuesto.
13	299	Llave de cajonera expuesta.
13	191	El equipo de cómputo se encuentra conectado a la corriente normal (toma blanca).
13	193.A	Ventilador portátil conectado a la toma regulada (naranja).
6	310	Impresora Zebra conectada a toma regulada (naranja).
6	356	Equipo todo en uno (pc) conectado a corriente normal (blanca).
6	367	Equipo todo en uno (pc) conectado a corriente normal (blanca).
6	361	Equipo todo en uno (pc) conectado a corriente normal (blanca).
6	397	Equipo todo en uno (pc) conectado a corriente normal (blanca).
6	372	Equipo de cómputo conectado a corriente normal (blanca).
6	424	Impresora conectada a corriente regulada (naranja).

Tabla N° 31. Elaboración propia. Fuente: Visita realizada a los pisos 6, 13 y 16 el día 20 de junio de 2023

Por otra parte, se informa que durante el recorrido se visitaron los centros de cableado de los pisos 6, 13 y 14, observando que dentro de estos se están almacenando elementos tales como cajas, tableros, papelería, equipos, madera, acrílicos, entre otros elementos. De acuerdo con lo sustentado, esta Oficina informa riesgos de disponibilidad en materia de seguridad de la información, por el posible daño que afecte el funcionamiento de equipos del ámbito tecnológico.

OBSERVACIÓN N° 30: Debilidades de control en el acceso al centro de cómputo de la Entidad:

Finalizando el recorrido por el centro de cómputo de la Entidad en el piso 14, se informa que la bitácora para registro de ingresos al centro de cómputo, no se está diligenciado efectivamente, debido a que en la línea de tiempo se evidenció un registro de diciembre de 2022 y el siguiente registro corresponde a mayo de 2023, es decir hay 5 meses aproximadamente donde no se realizó el diligenciamiento. También es importante mencionar que el formato de bitácora utilizado actualmente, no se encuentra oficializado en el sistema integrado de gestión de la Secretaría.

De acuerdo con lo expuesto en las tres observaciones, se están incumpliendo los siguientes ítems del manual y la política de seguridad y privacidad de la información así:

Política de Seguridad y Privacidad de la Información PO-GT-1 (3)

- Literal d del numeral 5.4.5 uso aceptable de los activos ": *En las sedes de la SDSCJ donde haya cableado estructurado, las tomas eléctricas ubicadas en las canaletas deberán ser usadas únicamente para la conexión de computadores, monitores o teléfonos IP. Los computadores deben ser conectados en las tomas naranjas y en ninguna circunstancia se puede conectar otros elementos eléctricos a los asignados en dichas tomas."*

Manual de Seguridad y Privacidad de la información MA-GT-01

- Numeral 5.7.2. "*El ingreso a los centros de cableado en las diferentes áreas será con el aval de la Dirección de Recursos Físicos y Gestión Documental. para lo cual, la Dirección de Tecnologías y Sistemas de la Información o la persona que se delegue mediante correo electrónico, solicitará la autorización de ingreso de usuarios permanente y/o temporal a dichos cuartos para actividades de soporte tecnológico que se requiera, el ingreso debe estar registrado mediante una bitácora con la siguiente información: a. Nombre completo de quien realiza el ingreso. b. Fecha de ingreso. c. Actividad a realizar. d. Tipo y número de documento. e. Administradora de Riesgos Laborales. f. Nombre de la empresa (si aplica). g. Nombre de la persona que hará el acompañamiento"*

- Numeral 5.7.7 ubicación y protección de los equipos describe que " *Los equipos de la Secretaría Distrital de Seguridad, Convivencia y Justicia tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aire acondicionado, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan información y/o brinden servicios de la Entidad, deben ser ubicados y protegidos estratégicamente dentro de las áreas disponibles que ofrezcan garantías de seguridad que prevenga la pérdida, daño o sustracción de información."*

- Literal c del numeral 5.7.9. titulado seguridad del cableado el cual describe "*Proteger el cableado de humedad o exposición a fuentes de calor que puedan afectar o generar daños a la estructura del mismo.".*
- *Literal c del numeral 5.7.15 titulada Política de escritorio limpio y pantalla limpia, donde se describe que "Guardar documentos bajo llave y conservar escritorios libres de documentación"*

RECOMENDACIONES N° 37,38 y 39 para controles de acceso físico:

- Realizar validación del cumplimiento de los controles frente a los accesos y en general a lo establecido para los centros de cableado de la Entidad, tanto en el nivel central como en los equipamientos adscritos. Si el caso lo amerita, actualizar las reglas y controles dentro del Manual de Seguridad y Privacidad de la información de la Entidad.

- Generar una iniciativa en la cual se garantice la conexión física de los equipos de cómputo y las buenas prácticas asociadas, de cara a generar conciencia por parte del personal de la Entidad.

- Validar el funcionamiento y la operación de los controles utilizados actualmente para el ingreso de personal al centro de cómputo de la Entidad y si es el caso, actualizar la información en el Manual de Seguridad y Privacidad de la información.

Asignación de ambientes de trabajo para los sistemas de información de la Entidad:

El numeral 5.8.4 del Manual de Seguridad y Privacidad de la información de la Entidad titula lo siguiente: "*Separación de los ambientes de desarrollo, pruebas, y operación*" y describe que *"La Dirección de Tecnologías y Sistemas de la Información, a través del procedimiento interno PD-GT-16 "Gestión de Pruebas Tecnológicas", procedimiento interno PD-GT-17 "Ciclo De Vida de desarrollo de software" de la Entidad, adoptó los lineamientos para los ambientes separados de producción, pruebas y desarrollo, con el fin de garantizar la integridad de la información procesada, evitar interferencias en el desempeño, reducir los riesgos de acceso o cambios no autorizados en el ambiente de producción. ",* con relación a esto, el equipo auditor procedió a validar la información entregada por la DTSI respecto a la existencia de los 3 ambientes para todos los sistemas de información de la Entidad.

OBSERVACIÓN N° 31: Falta de completitud de ambientes de desarrollo, pruebas u operación para los sistemas de información de la Entidad tal y como lo define el numeral 5.8.4 del Manual de Seguridad y Privacidad de la información:

Una vez enunciado lo anterior, la observación radica en que NO todos los sistemas de información de la Entidad tienen los 3 ambientes mencionados, situación que fue informada en el informe de auditoría especial de nómina dentro del capítulo seguridad de la información (SIAP Tiene ambiente de desarrollo y pruebas integrado y o separado); adicionalmente y validado el reporte emitido por la DTSI sobre ambientes de los sistemas de información, no se está cumpliendo lo definido de acuerdo a lo establecido y para tal fin se exponen los siguientes casos:

- SIGA: Misma URL para los 3 ambientes.
- SIGEM: No hay información registrada para los ambientes de desarrollo y pruebas.
- SIRPA: Misma URL para los ambientes de desarrollo y pruebas.
- SIMBA: No hay información registrada para los ambientes de desarrollo y pruebas.
- CASA LIBERTAD: Misma Dirección IP para los ambientes de desarrollo y pruebas.
- CENTINELLA: No hay información registrada para los ambientes de desarrollo y pruebas.

Basados en lo expuesto, se está incumpliendo lo definido en el numeral 5.8.4 del manual de seguridad y privacidad de la información el cual titula *Separación de los ambientes de desarrollo, pruebas, y operación,* por tanto el equipo auditor informa que los sistemas de información al no contar con los ambientes requeridos para operación y funcionamiento, pueden presentar riesgos, integridad, confidencialidad y disponibilidad, principalmente donde los ambientes son compartidos en la misma infraestructura (servidor) y los datos de producción accedidos por el equipo de desarrollo.

RECOMENDACIÓN N° 40: Ejecutar una revisión y diagnóstico por parte de la DTSI, para establecer si todos los sistemas de información cuentan con los 3 ambientes estipulados y descritos en el manual de seguridad y privacidad de la información de la Entidad, para el correspondiente registro de la información en una fuente oficial de la Dirección, permitiendo ejecutar revisión y monitoreos de

manera periódica. Adicionalmente, ejecutar un plan de acción para que se garantice el cumplimiento de esta actividad en todos los sistemas de información de la Entidad tanto misionales como de apoyo.

Lineamientos y directrices sobre copias de seguridad de los sistemas de información:

El numeral 5.8.6 Respaldo de Información del Manual de Seguridad y Privacidad de la información describe en el literal b lo siguiente: La frecuencia y alcance de las copias de respaldo de la información se establece por los líderes de proceso, al igual que los periodos de retención y la criticidad de la información respaldada.

OBSERVACION N°32: Falta de definición de frecuencia y alcance de copias de respaldo por parte de los líderes de proceso:

Al validar el tema de copias de seguridad con la DTSI, el equipo auditor no obtuvo información donde los líderes de proceso de los sistemas de información hayan definido reglas, frecuencia, alcance, periodos de retención y criticidad de la información respaldada, incumpliendo lo establecido en el numeral 5.8.6 del manual de seguridad y privacidad la información de la Entidad, por tanto, se presentan riesgos de integridad y disponibilidad de la información, por el hecho de que los lideres funcionales de acuerdo a su concepto emitan parámetros y lineamientos frente al manejo de su información, dejando la responsabilidad a la DTSI.

RECOMENDACIÓN N° 41: Validar el cumplimiento de este numeral por parte de la DTSI, solicitando a los dueños de la información y líderes de proceso los datos y reglas relacionadas con las copias de seguridad o backup de los sistemas de información, teniendo en cuenta y aplicando las mejores prácticas de la industria en materia de seguridad de la información.

Gestión de vulnerabilidades técnicas para los componentes de TI de la Entidad:

La DTSI entrega al equipo auditor soportes de los análisis de vulnerabilidades realizados en las vigencias 2022 y 2023 y específicamente para la presente vigencia se evidencian documentación de los mencionados análisis para los siguientes componentes:

- Ethical Hacking de SIGA ejecutado en el mes de febrero.
- Router de ETB ejecutado en el mes de marzo.
- Kaspersky SIGA ejecutado en el mes de abril.
- SIGA ejecutado en el mes de mayo.

OBSERVACIÓN N° 33: Falta de ejecución de Gestión de vulnerabilidades técnicas para todas las soluciones tecnológicas de la Entidad:

De acuerdo con la documentación validada por el equipo auditor, se presenta la observación de auditoría debido a que no se ha realizado análisis de vulnerabilidades a todas las soluciones tecnológicas de la Entidad (incluyendo las soluciones que están operando en el C4) y tampoco se evidenció planes de remediación frente a las situaciones detectadas o informadas en cada ejercicio de análisis. Lo anterior, incumple lo establecido en el numeral 5.8.12 del manual de seguridad y privacidad de la información, denotando riesgos de seguridad de la información en los pilares disponibilidad y confidencialidad.

RECOMENDACIÓN N°42: Ejecutar un plan de acción coordinado por la DTSI con el fin de ejecutar los análisis de vulnerabilidades para todos los componentes del ámbito tecnológico de la Secretaría y derivado de cada proceso ejecutar los correspondientes planes de remediación tal y como lo estipula el manual de seguridad y privacidad de la información de la Entidad. Lo anterior debe quedar estimado para todas las vigencias posteriores.

Documentación para el desarrollo seguro de sistemas de información en la Entidad:

El Manual de Seguridad y Privacidad de la información versión 3 de la Entidad en el numeral 5.10.4 describe la Política de Desarrollo Seguro así: *"La Dirección de Tecnologías y Sistemas de la Información, de acuerdo a lo establecido en el procedimiento interno PD-GT-17 "Ciclo de Vida de Desarrollo de Software" de la Entidad, así mismo, desarrollará las siguientes actividades: a. Implementar el Manual de Desarrollo Seguro a cargo del grupo de Sistemas de Información en el desarrollo de software"* y específicamente el literal b) define " *Implementar el Manual de Desarrollo Seguro a cargo del grupo de Sistemas de Información en el desarrollo de software".* Para tal fin el equipo auditor solicita a la DTSI soporte o evidencia del mencionado manual, remitiendo un documento borrador titulado manual de desarrollo seguro.

OBSERVACIÓN N° 34: Ausencia de documento titulado desarrollo seguro descrito en el manual de seguridad y privacidad de la información:

Basado en lo expuesto por el equipo auditor, el literal a del numeral 5.10.4 del manual de seguridad y privacidad de la información relacionado con la elaboración del manual de desarrollo seguro se está cumpliendo parcialmente, puesto que este se encuentra en proceso de construcción a partir de la presente vigencia. No obstante, se mencionan riesgos de integridad, confidencialidad y disponibilidad de la información, por no tener el documento que guie y oriente al equipo desarrollador en la ejecución de sus funciones y actividades.

RECOMENDACIÓN N° 43: Continuar y priorizar la elaboración del documento manual de desarrollo seguro y surtiendo todo el proceso establecido por la Entidad para incorporarlo al sistema integrado de gestión. Se enfatiza respecto a la revisión y validación del contenido del documento por parte de todos los grupos e ingenieros relacionados en la ejecución de las actividades.

Plan de Contingencia Tecnológica de la Secretaría:

Se valida por parte del equipo auditor con la DTSI sobre la existencia del plan de contingencia tecnológica a lo cual se informó que está en proceso de construcción el documento borrador, no obstante, se está dependiendo de unas actividades institucionales (otras dependencias) relacionadas con el tema. Lo anterior se encuentra estipulado en los literales a y b del numeral 5.13. 1 titulado planificación de la continuidad de la seguridad de la información, adicionalmente el numeral 5.13.2 titulado Implementación de la continuidad de la seguridad de la información.

OBSERVACIÓN N° 35: Falta de Plan de Contingencia Tecnológica de la Entidad:

De acuerdo con el contexto realizado, la observación de auditoría se presenta por la inexistencia del plan de contingencia tecnológica descrito el literal b del numeral 5.13.1 dentro del manual de seguridad y privacidad de la información, lo cual impacta el desarrollo y ejecución de las actividades en todas las dependencias de la Entidad, al momento de presentarse una situación adversa que

afecte la continuidad de las operaciones, así como también se generen riesgos de disponibilidad de la información, por el no acceso a los recursos de TI y sistemas de información.

RECOMENDACIÓN N°44: Continuar y priorizar el desarrollo de la iniciativa encaminada a la elaboración del plan de contingencia tecnológica de la Secretaría. Complementariamente coordinar con la Oficina Asesora de Planeación las actividades a ejecutar con la correspondiente estimación de los recursos requeridos para alinearlo con el plan de continuidad del negocio.

Procedimientos mencionados dentro del Manual de Seguridad y Privacidad de la Información sin encontrarse formalizados dentro del Sistema Integrado de Gestión:

Una vez revisado el manual de seguridad y privacidad de la información versión 3 de la Entidad, se identifica que a lo largo del documento se mencionan procedimientos no formalizados dentro del sistema integrado de gestión dentro de los cuales se encuentran:

- Procedimiento para la gestión de medios removibles en el numeral 5.4.8
- Procedimiento para el trabajo en áreas seguras numeral 5.7.5
- Procedimiento interno PD-GT-9 “Préstamo de Equipo de Tecnología” en el numeral 5.7.11
- Procedimiento interno PD-GT-10 “Cambio y/o alistamiento de Equipos” 5.7.10

OPORTUNIDAD DE MEJORA 9: Procedimientos mencionados dentro del manual de seguridad y privacidad de la información sin estar formalizados dentro del sistema integrado de gestión:
La Oficina de Control Interno informa la oportunidad de mejora debido a la mención de “*procedimientos”* dentro del manual de privacidad y seguridad de la información sin encontrarse formalizados ni oficializados en el SIG – MIPG. Lo anterior indica la falta de coherencia en el uso de términos y conceptos correspondientes al sistema integrado de gestión, generando riesgos de omisiones en la ejecución de las actividades de los procedimientos por parte del personal responsable.

RECOMENDACIÓN N° 45: Validar por parte de la DTSI con acompañamiento de la Oficina Asesora de Planeación - OAP el uso del término procedimientos dentro del manual de seguridad y privacidad de la información y para los casos que se estime y aplique, proceder con la creación del correspondiente procedimiento

4 CONCLUSIONES

Una vez culminado el trabajo de auditoría y revisado el proceso Gestión de Tecnologías de la Información, específicamente los procedimientos seleccionados de manera aleatoria se llegan a la conclusión general que el ámbito tecnológico de la Secretaría De seguridad, Convivencia y Justicia opera dentro de parámetros en idóneas condiciones.

Por medio de la gestión encabezada por de la Dirección de Tecnologías y Sistemas de la Información, se han identificado y abordado continuamente acciones, actividades, estrategias y planes en pro de la optimización y automatización de los procesos y procedimientos, sin dejar a un lado los temas de riesgos, seguridad digital y seguridad de la información, Modelo Integrado de Planeación y Gestión MIPG entre otros aspectos, por medio de la implementación de medidas de control.

Como se ha mencionado, la Entidad tiene un enfoque proactivo hacia la seguridad de la información, el manejo de riesgos, la gestión de proyectos, con lineamientos, procesos de capacitación y sensibilización adecuados dirigidos a todo el personal que se encuentra tanto en la sede central como en sus equipamientos o sedes adscritas, lo anterior buscando proteger los datos en todos sus niveles y prevenir posibles brechas de seguridad. Se han implementado mecanismos de respaldo y recuperación de datos, lo que garantiza la disponibilidad y la integridad de la información en caso de fallos técnicos. Todo esto bajo la línea que brinda el plan estratégico de tecnologías de la información PETI oficial de la Entidad.

Las soluciones tecnológicas contempladas dentro del catálogo de sistemas de información se encuentran operando y hasta el momento brindan soporte y mejora a las actividades diarias, apuntando a la optimización de los recursos disponibles. También se hace énfasis en la continua gestión de la infraestructura tecnológica que actualmente está implementada por medio del personal encargado de dichas labores.

Ahora bien, producto de las observaciones y oportunidades de mejora presentadas en el presente informe de auditoría, se identificaron temas de suma importancia en los que se pueden realizar mejoras, permitiendo el fortalecimiento del proceso por medio de la aplicación de planes de mejoramiento concisos y que apunten a atender la causa raíz que originaron las situaciones presentadas. Complementariamente se exponen las recomendaciones que pueden abarcar aspectos como la optimización en el desarrollo de sistemas, el cumplimiento de lo estipulado en el Sistema Integrado de Gestión, el fortalecimiento de los controles, la gestión de proyectos, la administración y gestión de la plataforma tecnológica y la mejora y el aumento de la cultura en materia de seguridad digital y seguridad de la información.

Dentro de los aspectos más notables a resaltar sobre los cuales la Secretaria debe enfocar esfuerzos y desarrollar iniciativas, mencionamos seguridad de la información, seguridad digital, ciberseguridad, uso y apropiación, proyectos de tecnología, desarrollo e integración de sistemas y aplicaciones, continuidad del negocio, documentación y principalmente la interacción y apropiación de los sistemas de información que operan en el C4, por tanto, se recomienda continuar monitoreando y actualizando constantemente el entorno tecnológico para mantenerse al día con los avances y las mejores prácticas en el campo. También se sugiere realizar revisiones y monitoreos periódicos de con las correspondientes evaluaciones de riesgo para adaptarse a las nuevas amenazas y mantener la confidencialidad, integridad y disponibilidad de los datos.

5 RECOMENDACIONES

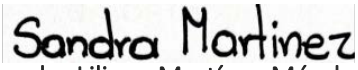
Las recomendaciones que genera la Oficina de Control Interno se encuentran asociadas a cada observación y oportunidad de mejora presentada a lo largo del presente documento.

.

Elaboró

Diego Alexander Urazán Franco
Auditor Líder-Contratista Oficina de Control Interno

Katherine Bolagay Gaitán
Contratista Oficina de Control Interno



Sandra Liliana Martínez Méndez
Contratista Oficina de Control Interno

Revisó y Aprobó

Karol Andrea Parraga Haché
Jefe Oficina de Control Interno