Nombre del informe
SEGUIMIENTO A LA GESTIÓN DEL RIESGO EN LA SECRETARÍA DISTRITAL DE PLANEACIÓN.

Área(s) Auditada(s) - Responsable(s)	Subsecretarios, Directores, Subdirectores y Jefes de Oficina

1. Objetivo

Verificar la gestión integral de riesgos en la Secretaría Distrital de Planeación en cumplimiento de la normatividad vigente y la aplicación de la política establecida por la entidad.

2. Alcance

Gestión integral de administración de riesgos, contemplando los riesgos operacionales (gestión), riesgos de corrupción, riesgos de seguridad de la información, Sistema de Administración del Riesgo de Lavado de Activos y Financiación al Terrorismo (SARLAFT), riesgos ambientales y riesgos asociados al Sistema de Seguridad y Salud en el Trabajo en la Secretaría Distrital de Planeación con corte al 30 de abril de 2024.

3. Criterios

- Decreto 124 del 26 de enero de 2016 *"Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano". Artículo 2.1.4.2. Mapa de Riesgos de Corrupción. Señálense como metodología para diseñar y hacer seguimiento al Mapa de Riesgo de Corrupción de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el documento "Guía para la Gestión del Riesgo de Corrupción".*
- Decreto 612 de abril 04 de 2018, *"por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado."* Art 1. "2.2.22.3.14**.** *Integración de los planes institucionales y estratégicos al Plan de Acción.*
- Norma Técnica colombiana NTC – ISO 9001
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6, expedida por Departamento Administrativo de la Función Pública (DAFP) noviembre de 2022. Se mantiene estructura conceptual para la administración del riesgo. Se incluye capítulo específico sobre riesgo fiscal.
- Política de Administración del Riesgo (E-LE-030): versión 18 de agosto de 2022.
- Instructivo de Administración del Riesgo (E-IN-005): versión 9 de agosto de 2023.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (A-LE-505), versión 3 de enero de 2024.
- Guía para la Gestión de Activos de Información de la SDP A-IN-016, Versión 10 de 2022
- Instructivo para identificación de peligros y valoración de riesgos para el Sistema de Gestión de la Seguridad y Salud en el Trabajo (A-LE-350) Versión 4 de 2023.
- Plan Institucional de Gestión Ambiental (A-LE-023) Versión 6 marzo 2021.
- Mapas de Riesgos y demás documentos del Sistema de Gestión asociados

4. Resultados del informe

4.1 Recolección de información y riesgos Identificados en el Seguimiento

Para el presente seguimiento mediante correo del 31 de mayo de 2024 se realizó solicitud de información vía correo electrónico a través de un cuestionario, del que se recibe respuesta el 7 de junio de 2024, adicionalmente, se realizó reunión con la Dirección Administrativa el 17 de julio de 2024 y como resultado se remite información vía correo electrónico ese mismo día.

Dentro de los riesgos y limitantes identificados en desarrollo de este seguimiento se presentan los siguientes:

- No fue posible la verificación de los Planes Operativos Anuales (POA) de vigencias anteriores, dado que el Sistema Integrado para la Planeación y Gestión (SIPG) no permitió la consulta.
- Posibles inconvenientes se pueden presentar en el manejo de la documentación oficial, dado que algunos archivos oficiales que fueron suministrados por las diferentes áreas consultadas fueron anexados en formatos editables tales como Word y Excel. Adicionalmente, para algunas dependencias se observaron debilidades en el manejo y custodia de la información.
- La consulta de los reportes del monitoreo a los riesgos de primera línea de defensa, así como sus evidencias, no son fácilmente consultables, dado que se reportan a la Dirección de Planeación Institucional sin que exista aplicativo o repositorio con la información respectiva.

4.2 Contexto General Gestión Integral de Riesgos

La Política de Administración del Riesgo (E-LE-030) es extensiva a todos los procesos desarrollados por la Secretaría Distrital de Planeación y debe ser cumplida por todos los servidores y contratistas de la entidad independientemente su nivel jerárquico, y desarrollada a través de los diferentes mapas y planes de tratamiento para los siguientes tipos de riesgos:

- Riesgos de gestión: riesgos operativos que pueden afectar el logro de los objetivos de los procesos estratégicos, misionales, de apoyo y de evaluación que conforman el Sistema de gestión.
- Riesgos de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Riesgos de seguridad de la información: se encuentran alineados a la pérdida de integridad, confidencialidad y disponibilidad de la información, aplicable a todos los procesos de conformidad con el alcance del Modelo de seguridad y privacidad de la información.

La Secretaria Distrital de Planeación establece la metodología para la administración de los riesgos previstos en esta política a través de los documentos que hacen parte del Sistema de Gestión y que toman como marco de referencia para los riesgos de gestión y de seguridad de la información, los lineamientos de la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas" proferida por el DAFP en su última versión 6 de noviembre de 2022 y para los riesgos de corrupción, la Guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el DAFP.*

Por otra parte, se cuenta con el Instructivo para la Gestión del Riesgo E-IN-005 el cual considera que la gestión del riesgo es un proceso efectuado por la Alta Dirección y por todo el personal de la entidad, con el propósito de proporcionar a la administración un aseguramiento razonable para el logro de los objetivos institucionales, los principales beneficios de la administración del riesgo para la entidad son los siguientes:

- Apoyo en la toma de decisiones en los diferentes niveles de la organización.
- Incremento de la capacidad de la entidad para alcanzar sus objetivos.
- Apoyo para la operación normal de la organización.
- Identificación de acciones para minimizar la probabilidad e impacto de los riesgos.
- Mejoramiento en la calidad de los procesos y sus servidores (calidad se trata de forma paralela con riesgos).
- Fortalecimiento de la cultura de control de la organización.
- Brinda herramientas y controles a la entidad para hacer una administración más eficaz y eficiente.

La Oficina de Control Interno indagó sobre cómo se determinó el apetito, la tolerancia y la capacidad de Riesgo para la Secretaria Distrital de Planeación, para lo cual la Dirección de Planeación Institucional informa que "*La definición del apetito de riesgo se realizó bajo un enfoque cualitativo y se estableció para los riesgos de gestión, tomando como base la autonomía de la Entidad para delimitarlo de esta forma, buscando que los procesos puedan aceptar los riesgos ubicados en el nivel bajo con una adecuada implementación de controles y un monitoreo que les permita identificar cambios en el contexto que requieran una actualización en la valoración de los riesgos. Por otra parte, la tolerancia del riesgo, entendiéndola como la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo, se estableció desde el nivel de riesgo moderado a alto y por último, la capacidad del riesgo, vista como el máximo nivel de riesgo que la Secretaría podría soportar, se estableció desde el nivel bajo al nivel extremo; lo anterior tuvo como base que aún en el nivel extremo existen opciones de tratamiento como transferirlo, suspender la acción que genera el riesgo o desarrollar planes de acción robustos que lo reduzcan y así evitar que se comprometa el cumplimiento de los objetivos de la SDP*."

La Oficina de Control Interno recomienda que en la Política de Administración del Riesgo (E-LE-030) contengan una integralidad en sus riesgos por tipología como Continuidad del negocio, Contingentes, Legales, Lavado de Activos y Financiación del terrorismo SARLAFT, Seguridad y Salud en el Trabajo, Ambientales y Fiscales.

Por otra parte, se indagó sobre la existencia de documento y/o lineamiento vigente para reportar posibles eventos de riesgo, para lo cual se indicó que en los mapas de riesgos se encuentra el campo para reportar las materializaciones de riesgos y las evidencias de las acciones adelantadas (última hoja de cálculo del archivo). Teniendo en cuenta que no se han reportado eventos para el periodo de seguimiento no se adjuntan evidencias.

La Dirección de Planeación Institucional realizó sesión de sensibilización en la gestión del riesgo con los diferentes procesos, en la cual se trataron entre otros temas, la política de riesgos y demás documentos asociados, adjuntando como evidencia la presentación y listas de asistencias de noviembre de 2023 de la socialización de los resultados de la auditoría ICONTEC y sensibilización gestión del riesgo.

4.2.1 Gestión del cambio (rediseño, Gestiónate)

Dados los cambios que se han generado en los últimos años en la entidad, tales como el rediseño institucional, cambio de aplicativos utilizados, Plan de Ordenamiento Territorial (POT), entre otros,

la Oficina de Control Interno incluyó dentro del presente seguimiento, el análisis a la *Planificación de los Cambios* de que trata el numeral 6.3 de la Norma Técnica Colombiana NTC-ISO 9001, y los riesgos relacionados a estos procesos, cuya materialización puede afectar el cumplimiento de la misión institucional en la entidad.

Dentro del proceso E-CA-001 *Direccionamiento estratégico*, se tiene estructurado el procedimiento E-PD-025 *Identificación, implementación y seguimiento de la gestión del cambio*, que en su versión 3 de noviembre de 2023 fija como objetivo "*Establecer los lineamientos necesarios para identificar, analizar, implementar, realizar seguimiento y controlar los cambios que puedan afectar el cumplimiento de los objetivos de la entidad, su desempeño institucional y la entrega de productos y/o servicios a la ciudadanía y partes interesadas.",* así como su alcance *"Inicia con la identificación de la necesidad de establecer un cambio que afecta el cumplimiento de los objetivos de la entidad, su desempeño institucional y la entrega de productos y/o servicios a la ciudadanía y partes interesadas, continúa con el establecimiento de un plan de trabajo para la implementación del cambio y termina con el seguimiento realizado a la ejecución de las actividades definidas en el plan de trabajo y el respectivo plan de mejoramiento cuando así se requiera. Este procedimiento aplica para todos los procesos de la entidad."*

Atendiendo lo anterior, se indagó a la Dirección de Planeación Institucional (DPI) como líder del procedimiento, sobre la forma cómo se desarrolla en la Entidad, aplicado en temas estratégicos que puedan llegar a afectar el cumplimiento de los objetivos de la SDP.

Indicó el área encargada, que la gestión del cambio en la entidad se viene documentando a través del documento *Planificación de los cambios que afecten el cumplimiento de los objetivos de la* SDP E-FO-056, en lo relacionado con aquellos cambios que pueden llegar a afectar la operatividad y sostenibilidad del Sistema de Gestión y los objetivos institucionales de la entidad. Es así que, revisados los soportes remitidos, en el Acta N. 5 de sesión ordinaria del Comité Institucional de Gestión y Desempeño (CIGD) del 29 de abril de 2022, dentro del capítulo *Cambios en las Cuestiones Externas e Internas del Sistema de Gestión,* se hace mención a 5 situaciones que pueden afectar el sistema:

Tabla N. 1. Planificación de cambios potenciales

No.	ASPECTO	1. PLAN ORDENAMIENTO TERRITORIAL		2.PLANEACIÓN ESTRATÉGICA		3.CAMBIOS EN EL CÓDIGO DISCIPLINARIO		4. NUEVA METODOLOGÍA DE RIESGOS		5. REDISEÑO INSTITUCIONAL		SUBTOTAL	
	PREGUNTA	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	¿El cambio implica modificaciones al plan estratégico?	SI			NO		NO	SI		SI		3	2
2	¿Impacta el cumplimiento de una meta de Plan de Desarrollo?	SI			NO		NO		NO		NO	1	4
3	¿Impacta la prestación de productos y/o servicios de la entidad?	SI		SI		SI			NO	SI		4	1
4	¿Modifica las funciones y/o responsabilidades?	SI			NO	SI		SI		SI		4	1
5	¿Es necesario modificar la Política y los Objetivos de la calidad?	SI		SI			NO	SI		SI		4	1
6	¿Es necesario modificar el Mapa de Procesos?	SI			NO	SI			NO	SI		3	2
7	¿Es necesario modificar el objetivo o alcance de algún proceso?	SI		SI		SI		SI		SI		5	0
8	¿Es necesario modificar las actividades, las secuencias o las interacciones de algún proceso?	SI		SI		SI		SI		SI		5	0
9	¿Es necesario ajustar los parámetros de control o mecanismo de seguimiento, medición, análisis y evaluación de algún proceso?	SI		SI		SI		SI		SI		5	0
10	¿Es necesario contratar externamente algún proceso, producto y/o servicio?	SI		SI		SI			NO		NO	3	2
11	¿Es necesario programar formación al personal involucrado?	SI		SI		SI		SI		SI		5	0
12	¿Se requiere actualizar el mapa de riesgos de algún proceso e identificar nuevos controles?	SI		SI		SI		SI		SI		5	0
	SUBTOTAL	12		8		9		8		10			

Fuente: Acta N. 5 CIGD del 29 de abril de 2022

En el Acta N. 6 del 4 de mayo de 2022, se indica que para los temas 1, 3 y 4, se presentará la información referente a la gestión del cambio, el 31 de marzo de 2023 y frente al rediseño institucional para el 30 de junio de 2023.

En el Acta N. 7 del 15 de junio de 2022, se aprobó la gestión del cambio referente al cambio del Código General Disciplinario, para lo cual se anexa el documento diligenciado E-FO-056 *Planificación de los cambios que afecten el cumplimiento de los objetivos de la SDP* con el plan de trabajo definido. Al respecto se observa que en el plan de trabajo se citan actividades que iniciaron en noviembre de 2021, es decir, anterior a la aprobación de la gestión del cambio.

En el Acta N. 11 del 21 de diciembre de 2022, se aprueba la Gestión del cambio propuesta para el tema relacionado con el Plan de Ordenamiento Territorial. Para tal fin se anexa diligenciado el E-FO-056. En el formato se evidencia que el plan de trabajo inició en diciembre de 2021, es decir un año antes de la aprobación de la gestión del cambio. Al respecto, se observa que en el campo *Riesgos asociados al cambio* se incluyen los riesgos definidos para el proceso y no los riesgos asociados en los cambios identificados y decidir si dichos riesgos son o no aceptables.

En el Acta N. 2 del 26 de abril de 2023, en el capítulo *Estado de las Decisiones Tomadas en la Reunión de Revisión por la Dirección*, se aprueba el formato E-FO-056 para el Rediseño Institucional, aunque en el formato se hace mención que fue tratado en sesiones del 29 de abril y 4 de mayo de 2022 del Comité Institucional de Gestión y Desempeño (CIGD). Llama la atención que, aunque este proceso inició en la vigencia 2022, la aprobación de la gestión del cambio se registra en Acta de CIGD de abril de 2023. Asimismo, se observan acciones que no se cumplieron en el tiempo establecido, entre las que se citan:

- Matriz de Equivalencias construida en conjunto con las áreas Dirección de Planeación Institucional, programada para noviembre de 2022 y oficializada en el Sistema de Gestión el 24 de octubre de 2023.
- Fichas de caracterización revisadas y aprobadas por líderes de procesos proyectada para diciembre de 2022. Sin embargo, a marzo de 2024 se estaban realizando las actualizaciones definitivas de las caracterizaciones de procesos de acuerdo con memorando 3-2024-09339 emitido por la Dirección de Planeación Institucional.

Referente a la gestión del cambio relacionado con el Software para el sistema de Gestión "Gestiónate - ISolucion" y el nuevo Plan Distrital de Desarrollo "Bogotá Camina Segura", la Dirección de Planeación Institucional indicó que el E-FO-056 será aprobado en el marco de la Revisión por la Dirección de la vigencia 2023, la cual se llevará a cabo entre los meses de junio y julio de 2024.

Del análisis anteriormente descrito, la Oficina de Control Interno observa una oportunidad de mejora en el manejo de la Gestión del Cambio en la entidad, siendo necesario el fortalecimiento de su planificación, a fin de disminuir los impactos negativos que se puedan generar por su implementación, atendiendo lo establecido en la norma NTC ISO 9001:2015 que en su numeral 6.3 señala: *"La organización debe considerar: a) el propósito de los cambios y sus consecuencias potenciales; b) la integridad del sistema de gestión de la calidad; c) la disponibilidad de recursos; d) la asignación o reasignación de responsabilidades y autoridades."*. Por lo anterior, se recomienda que la planificación y aprobación de la gestión de cambios se realice con anterioridad a su implementación, de acuerdo con lo definido en las acciones 2 a 7 del E-PD-025 *Identificación, implementación y seguimiento de la gestión del cambio,* Referentes a *Identificar la necesidad de establecer un cambio, Presentar y aprobar la*

propuesta del cambio por parte del Comité Institucional de Gestión y Desempeño, incluir actividades en el Plan Operativo Anual e iniciar la implementación.

En cuanto a la inclusión de las actividades en el Plan Operativo Anual (POA) no fue posible su verificación dado que el Sistema Integrado para la Planeación y Gestión (SIPG) no permitió la consulta de la información para la vigencia 2022.

Adicionalmente, se sugiere que el almacenamiento de la documentación que soporta la gestión del cambio se realice en formatos que no permitan su modificación, una vez sean aprobados por instancias decisorias de la entidad, atendiendo a que los formatos suministrados se encontraban en archivos Word.

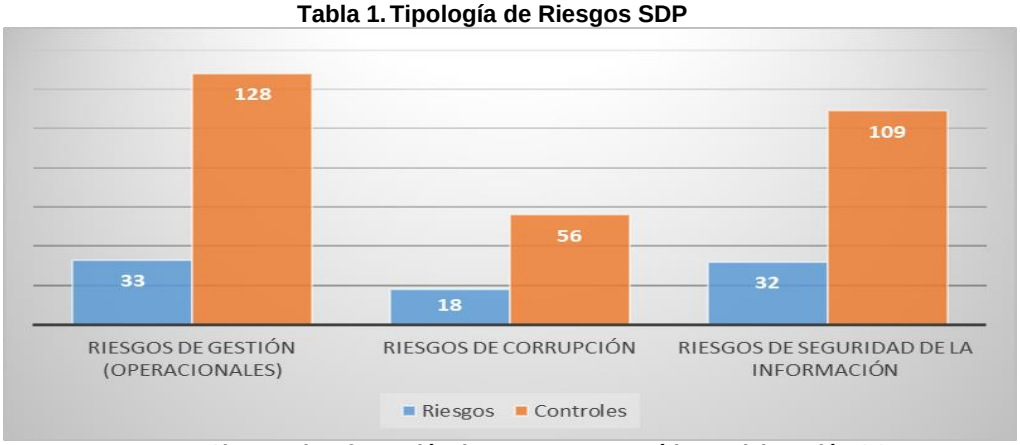
4.2.2 Caracterización de los riesgos de acuerdo con la Política de administración del riesgo

Para el seguimiento de los riesgos contemplados en la *Política de Administración del Riesgo* (E-LE-030) de la Secretaría Distrital de Planeación, la Oficina de Control Interno tomó como base los mapas de riesgos por proceso vigentes que reposan en el Sistema de Información de Procesos Automáticos (SIPA) para cada uno de los 15 procesos existentes a la fecha de este seguimiento.

Verificado el *Mapa de Riesgos Institucional* E-LE-017 Versión 24 de junio de 2023, publicado en el SIPA, la información no se encuentra actualizada para cada uno de los riesgos según su clasificación (Gestión, Corrupción y de Seguridad de la Información). conforme a los reajustes o actualizaciones realizados por cada proceso durante esta vigencia, los cuales se detallan más adelante.

La siguiente gráfica muestra que el 40% de los riesgos corresponde a la tipología Gestión, seguido del 39% correspondiente a riesgos de seguridad de la información y un 22% a riesgos de corrupción, a los cuales se les estructuraron 293 controles principalmente a riesgos de gestión:

Tabla 1. Tipología de Riesgos SDP



Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI

Se han identificado 83 riesgos y 293 controles por cada tipología los cuales se analizarán a continuación:

4.2.2.1 ADMINISTRACIÓN DEL RIESGOS DE GESTIÓN

La Secretaría Distrital de Planeación se encuentra actualizando los diferentes mapas de riesgos de gestión al interior de la entidad, para lo cual se consultó en el Sistema de Información de Procesos Automáticos (SIPA) cada uno de los documentos y actos que a continuación se relacionan teniendo en cuenta el código, la fecha de actualización y el número de acta de cada proceso así:

Tabla N. 2. Actualización Mapas de Riesgo de Gestión

	Proceso	Código	Fecha	Acta #
1	Administración de Recursos Físicos y Servicios Generales	A-LE-311	30/01/2024	41
2	Administración del Talento Humano	A-LE-306	7/02/2024	78
3	Contratación de Bienes y Servicios	A-LE-304	30/04/2024	183
4	Control Interno Disciplinario	S-LE-028	31/01/2024	64
5	Coordinación de Políticas Públicas y de Instrumentos de Planeación	M-LE-137	31/01/2024	68
6	Direccionamiento Estratégico	E-LE-047	12/02/2024	88
7	Evaluación y Control	S-LE-014	8/02/2024	85
8	Gestión de Recursos Financieros	A-LE-305	30/01/2024	44
9	Gestión Documental	A-LE-312	30/01/2024	40
10	Mejoramiento Continuo	S-LE-013	12/02/2024	89
11	Participación y Comunicación	E-LE-048	8/03/2024	148
12	Planeación Territorial y Gestión de sus Instrumentos	M-LE-132	30/11/2023	482
13	Producción, Análisis y Divulgación de la Información	M-LE-164	9/02/2024	86
14	Soporte Legal	A-LE-456	21/02/2024	107
15	Soporte Tecnológico	A-LE-303	31/01/2024	70

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Se puede observar que los mapas de gestión fueron actualizados en esta vigencia 2024, a excepción del mapa de riesgos del proceso *Planeación Territorial y Gestión de sus Instrumentos* actualizado en noviembre de 2023.

Los riesgos de gestión identificados se clasifican según la Política así:

Tabla N. 3. Descripción para la Clasificación de Riesgo de Gestión

CATEGORÍA	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: E-LE-030 Política de Administración del Riesgo. Elaboración OCI.

Teniendo en cuenta la anterior descripción, en la Secretaría Distrital de Planeación los riesgos se clasifican como se muestra a continuación, alineado con el factor de riesgo, donde un 67% se refiere a la ejecución y administración de procesos correspondiente a 22 riesgos, seguidos de Usuarios, Productos y Prácticas con un 27% correspondiente a 9 Riesgos identificados.

Tabla N. 4. Clasificación de Riesgo de Gestión SDP

Clasificación del Riesgo	Alineación con Factor de Riesgo	Cantidad	%
Ejecución y Administración de procesos	Procesos	22	67%
Usuarios, productos y prácticas, organizacionales	Procesos, Evento Externo, Talento Humano, Tecnologías e Infraestructura	9	27%

Clasificación del Riesgo	Alineación con Factor de Riesgo	Cantidad	%
Fallas Tecnológicas	Tecnología	1	3%
Daños Activos Físicos	Infraestructura Evento externo	1	3%
Total		**33**	**100%**

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Por otra parte, se presenta una frecuencia o periodicidad con la que se ejecutan las actividades asociadas al riesgo, las cuales impactan en los niveles de probabilidad y se relacionan a continuación, donde el 30% refiere controles permanentes, seguidos de aquellos mensuales que representan el 24% y actividades diarias con un 18%:

Tabla N. 5. Frecuencia de Riesgo de Gestión SDP

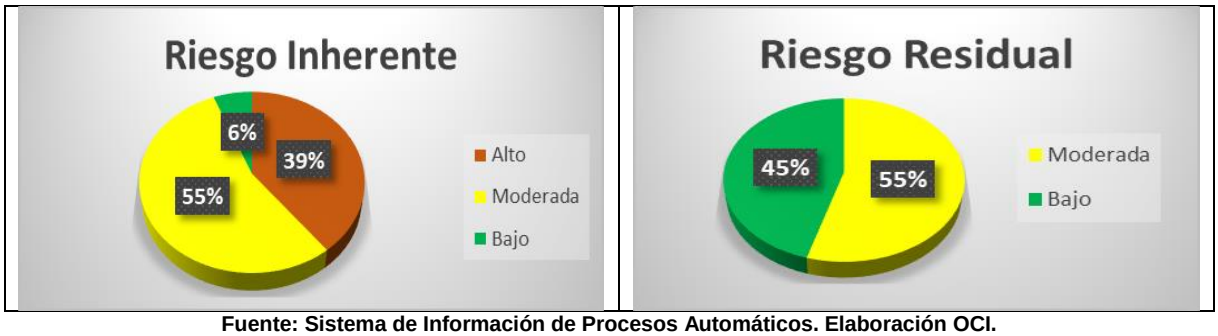
Frecuencia con la cual se realiza la actividad	Cantidad	%
Permanente	10	30%
Diaria	6	18%
Semanal	1	3%
Quincenal	1	3%
Mensual	8	24%
Trimestral	3	9%
Anual	4	12%
Total	**33**	**100%**

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

En cuanto a la Evaluación del Riesgo de Gestión se puede evidenciar que, de los 33 riesgos, el riesgo Residual disminuye con respecto al Riesgo Inherente y desaparecen los riesgos altos debido a la valoración de los controles que se definen a continuación así:

Tabla N. 6. Evaluación del Riesgo de Gestión SDP

Perfil de Riesgos de Gestión Consolidado SDP					
Riesgo Inherente	**TOTAL**	**%**	**Riesgo Residual**	**TOTAL**	**%**
Alto	13	39%	Alto	0	0%
Moderada	18	55%	Moderada	18	55%
Bajo	2	6%	Bajo	15	45%
TOTAL	33	100%	**TOTAL**	33	100%



Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Respecto a la valoración de los 128 controles con los atributos de eficiencia e informativos que están relacionados con la formalidad del control a través de variables cualitativas, así:

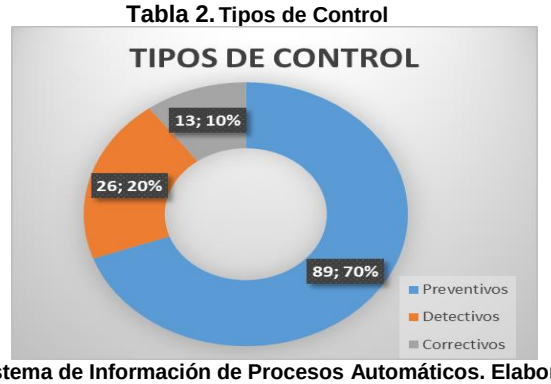
Tabla N. 7. Valoración de los controles del Riesgo de Gestión SDP

Proceso		#Control	Atributos de Eficiencia	
			Tipo de Control	Implementación
1	Administración de Recursos Físicos y Servicios Generales	5	3 Preventivo, 2 Detectivos	5 Manuales
2	Administración del Talento Humano	18	13 Preventivos, 5 Detectivos	18 Manuales
3	Contratación de Bienes y Servicios	12	9 Preventivos, 3 Correctivos	12 Manuales
4	Control Interno Disciplinario	4	2 Preventivo, 2 Detectivos	4 Manuales
5	Coordinación de Políticas Públicas y de Instrumentos de Planeación	8	4 Preventivos, 1 Detectivo, 3 Correctivos	7 Manuales ,1 Automático
6	Direccionamiento Estratégico	6	3 Preventivos, 3 Detectivos	6 Manuales
7	Evaluación y Control	4	4 Preventivos	3 Manuales
8	Gestión de Recursos Financieros	8	8 Preventivos	8 Manuales
9	Gestión Documental	4	2 Preventivo, 2 Detectivos	3 Manuales
10	Mejoramiento Continuo	3	2 Preventivos, 1 Detectivo	3 Manuales
11	Participación y Comunicación	7	4 Preventivos, 1 Detectivo, 2 Correctivos	7 Manuales
12	Planeación Territorial y Gestión de sus Instrumentos	12	6 Preventivos, 4 Detectivos, 2 Correctivos	12 Manuales
13	Producción, Análisis y Divulgación de la Información	13	11 Preventivos, 2 Detectivos	10 Manuales ,1 Automático
14	Soporte Legal	2	1 Preventivo, 1 Detectivo,	2 Manuales
15	Soporte Tecnológico	22	17 Preventivos, 2 Detectivos, 3 Correctivo	26 Manuales
TOTALES		**128**		

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Se puede observar que 89 son preventivos correspondiendo al 70% del total de controles, 26 defectivos correspondientes al 20% y finalmente se identificaron 13 como correctivos con un 10% del total de los controles. De estos últimos, en el análisis por proceso que se detalla en el numeral 4.3, se observó que en algunos casos no corresponden a controles correctivos, dado que no se relaciona con la gestión en el evento de una materialización de riesgos. Por lo anterior, se recomienda la revisión y ajuste en la clasificación de este atributo.

Tabla 2. Tipos de Control



Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Por otra parte, según la forma en el que se ejecuta el control, el 98% de los controles son manuales ejecutados por personas, es decir 126 controles y 2 son automáticos ejecutados por un sistema o aplicativo correspondiente al 2% del total. Respecto al atributo informativo relacionado con la documentación de los controles, un 91%, es decir 119 se encuentran documentados y 9 sin documentar. Referente a la frecuencia de los controles, el 99% de los controles, es decir 127, registran frecuencia continua y se aplica siempre que se realiza la actividad que conlleva el riesgo, mientras que uno se ejecuta de manera aleatoria. Finalmente, el 95% de los controles registran evidencias del control y 7 se encuentran sin registro. Por lo cual se recomienda fortalecer los controles sin registro a fin de documentarlos.

4.2.2.2 ADMINISTRACIÓN DE RIESGOS DE CORRUPCIÓN

La Oficina de Control Interno adelantó la verificación de los mapas de riesgos de corrupción de cada uno de los procesos, abarcando la generalidad de los riesgos, sus causas y controles, registrados en el Sistema de Gestión de la entidad, aplicativo SIPA y publicados en la sede electrónica institucional. Se puede evidenciar que las matrices de riesgos de corrupción se actualizaron en su totalidad fueron en enero del presente año conforme a lo reportado en el aplicativo SIPA. De manera general, se le realizaron actualizaciones y/o modificaciones principalmente en la estructuración y redacción de los controles, de acuerdo con lo señalado en la guía de administración de riesgos y el diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública – Departamento Administrativo de la Función Pública (DAFP), actividades y fechas.

En cuanto a la identificación de Riesgos de Corrupción sus causas y controles, con corte al 30 de abril de 2024, se observa que la Secretaría Distrital de Planeación continua con 18 Riesgos de Corrupción, 55 causas y 56 controles para los 15 procesos de la entidad registrados en el SIPA.

Tabla N. 8. Identificación riesgos, sus causas y controles de corrupción por proceso

	PROCESO	RIESGOS	CAUSAS	CONTROLES
1	Administración de Recursos Físicos y Servicios Generales	1	2	2
2	Administración del Talento Humano	1	4	6
3	Contratación de Bienes y Servicios	2	2	9
4	Control Interno Disciplinario	1	2	2
5	Coordinación de Políticas Públicas y de Instrumentos de Planeación	1	4	2
6	Direccionamiento Estratégico	2	7	7
7	Evaluación y Control	1	3	2
8	Gestión de Recursos Financieros	1	2	3
9	Gestión Documental	1	3	1
10	Mejoramiento Continuo	1	2	2
11	Participación y Comunicación	1	5	3
12	Planeación Territorial y Gestión de sus Instrumentos	2	9	5
13	Producción, Análisis y Divulgación de la Información	1	6	7
14	Soporte Legal	1	2	3
15	Soporte Tecnológico	1	2	2
TOTALES		**18**	**55**	**56**

Fuente: Dirección de Planeación Institucional, publicación riesgos de corrupción página web SDP. Elaboración OCI.

Llama la atención, que dentro de los riesgos de corrupción definidos sólo uno se asocia a un trámite *Consulta de documentación urbanística* bajo el proceso de *Gestión Documental*. No se observa en los procesos misionales riesgos asociados a sus trámites, atendiendo a que en su definición propiamente dicha tiene implícita la relación con terceros, que puede implicar posibles hechos de corrupción. Por lo anterior, se recomienda el análisis de los trámites y Otros Procedimientos Administrativos a fin de identificar los posibles riesgos asociados, en concordancia con lo establecido en el Protocolo para la identificación de riesgos corrupción asociados a la prestación de trámites y servicios del Departamento Administrativo de la Función Pública, que entre otras cosas indica que *"El resultado de la identificación de riesgos de corrupción se debe constituir en un criterio para la priorización de los trámites a intervenir mediante estrategias de racionalización, bien sea mediante acciones normativas, administrativas o tecnológicas de racionalización.".*

La siguiente tabla registra la Evaluación de Riesgo (probabilidad e Impacto) de Corrupción por proceso, evidenciando que luego de establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto:

Tabla N. 9. Evaluación del Riesgo de Corrupción

PROCESO	RIESGOS	RIESGO INHERENTE	RIESGO RESIDUAL
Administración de Recursos Físicos y Servicios Generales	1	ALTO	ALTO
Administración del Talento Humano	1	ALTO	ALTO
Contratación de Bienes y Servicios	2	MODERADO	MODERADO
Control Interno Disciplinario	1	ALTO	ALTO
Coordinación de Políticas Públicas y de Instrumentos de Planeación	1	ALTO	ALTO
Direccionamiento Estratégico	2	EXTREMO	EXTREMO
Evaluación y Control	1	EXTREMO	EXTREMO
Gestión de Recursos Financieros	1	ALTO	ALTO
Gestión Documental	1	ALTO	ALTO
Mejoramiento Continuo	1	ALTO	ALTO
Participación y Comunicación	1	MODERADO	MODERADO
Planeación Territorial y Gestión de sus Instrumentos	2	ALTO	ALTO
Producción, Análisis y Divulgación de la Información	1	ALTO	ALTO
Soporte Legal	1	ALTO	ALTO
Soporte Tecnológico	1	EXTREMO	EXTREMO
TOTALES	**18**		

Fuente: Dirección de Planeación Institucional, publicación riesgos de corrupción página web SDP. Elaboración OCI.

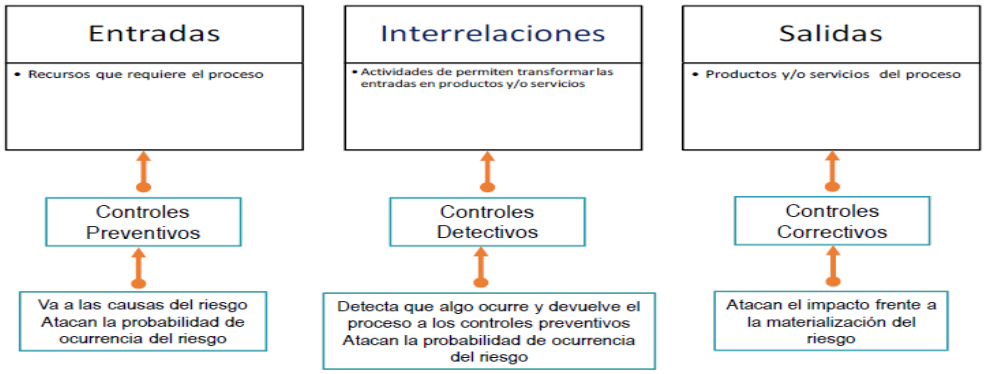
Se puede evidenciar que el 61% de los riesgos se encuentran clasificados como altos luego responder afirmativamente de 6 a 11 preguntas contempladas en la matriz de criterios señalado en la política de administración del riesgo, lo que genera altas consecuencias sobre la entidad y el 22% como extremos que genera consecuencias importantes para la entidad, por otra parte, retomando la definición de Nivel de riesgo (riesgo residual) como *"el resultado de aplicar la efectividad de los controles al riesgo inherente",* la Oficina de Control Interno evidenció que todos los riesgos residuales, sin excepción, permanecen en el mismo nivel que los inherentes ya descritos, pese a que se están administrando 56 controles. Lo anterior es una señal de alerta toda vez que el 83% de los riesgos están en los niveles extremo y alto, y allí permanecen, aunque se gestionen sus controles.

Dado lo anterior, la Oficina de Control Interno recomienda la revisión de los riesgos de corrupción y los controles establecidos para su tratamiento, considerando necesario tener en cuenta, entre otras cosas:

- Si hay deficiencias en aplicación de la metodología
- Si el impacto que tienen los controles sobre el riesgo no es lo suficientemente contundente, o
- Si los controles existentes son insuficientes.

Por otra parte, en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en su versión 6 emitida en noviembre 2022 por DAFP, establece *"la tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y , por lo tanto, establecer su tipología con mayor precisión"* así:

Tabla 3. Ciclo del Proceso y Tipologías de Controles



Fuente: Guía administración de riesgos Versión 6 DAFP

La entidad identificó 56 controles para los riesgos de corrupción, (entre 2 y 9 controles, como máximo por riesgo), que se encuentran en la tipologías descritas en la siguiente tabla, 37 controles Preventivos (*control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo*) correspondiente al 66%, 15 Detectivos (*control accionado durante la ejecución del proceso)* para un 27% y finalmente 4 correctivos (*control accionado en la salida del proceso y después de que se materializa el riesgo)* con un 7% del total de los tipos de controles:

Tabla N. 10. Análisis de Controles

	TIPO DE CONTROL			Total
PROCESO	**Preventivo**	**Detectivo**	**Correctivo**	
Administración de Recursos Físicos y Servicios Generales	0	2	0	2
Administración del Talento Humano	5	1	0	6
Contratación de Bienes y Servicios	7	0	2	9
Control Interno Disciplinario	1	1	0	2
Coordinación de Políticas Públicas y de Instrumentos de Planeación	1	1	0	2
Direccionamiento Estratégico	4	3	0	7
Evaluación y Control	1	1	0	2
Gestión de Recursos Financieros	3	0	0	3
Gestión Documental	1	0	0	1
Mejoramiento Continuo	1	1	0	2
Participación y Comunicación	2	0	1	3
Planeación Territorial y Gestión de sus Instrumentos	1	4	0	5
Producción, Análisis y Divulgación de la Información	7	0	0	7
Soporte Legal	1	1	1	3
Soporte Tecnológico	2	0	0	2
TOTALES	**37**	**15**	**4**	**56**
%	**66%**	**27%**	**7%**	

Fuente: Dirección de Planeación Institucional, publicación riesgos de corrupción página web SDP. Elaboración OCI

De acuerdo a la tabla 10. los controles son marcados como preventivo, aunque 2 de los 15 procesos no cuentan con este tipo de controles. Así mismo, los controles correctivos solo fueron considerados por 3 de los 15 procesos. Por otra parte, se evidenció que las matrices de riesgos de corrupción no incluyen información sobre la ejecución del control, si es manual ejecutado por personas o automático por un sistema, por lo que se recomienda incluir dentro de los atributos de eficiencia para el diseño de los controles el interrogante sobre si la implementación de los controles se realiza de forma automática o manual, conforme a lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

Para la valoración y el análisis de los controles la Secretaría Distrital de Planeación toma como referente lo indicado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018, emitida por el DAFP, la cual establece estos 7 interrogantes para la valoración de los controles frente a la mitigación del riesgo, y como consecuencia de esta evaluación se encuentra en el rango de calificación **FUERTE**, de acuerdo con la calificación realizada por cada proceso y el control se ejecuta de manera consistente por parte del responsable. Por lo anterior, y dadas las observaciones a los mapas de riesgos de corrupción por cada proceso que se establecen en el numeral 4.3, se recomienda la revisión de las respuestas dadas en esta valoración, ya que en algunos casos no es acorde con la realidad de los controles.

Tabla N. 11. Valoración de Controles

DISEÑO DEL CONTROL	VALORACIÓN DEL CONTROL
¿Existe un responsable asignado a la ejecución del control?	ASIGNADO
¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	ADECUADO
¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	OPORTUNA
¿Las actividades que se desarrollan en el control realmente buscan por si solas prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	PREVENIR O DETECTAR
¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	CONFIABLE
¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE
¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	COMPLETA

Fuente: Dirección de Planeación Institucional, publicación riesgos de corrupción página web SDP. Elaboración OCI

4.2.2.3 ADMINISTRACIÓN DEL RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar el seguimiento a los riesgos de seguridad de la información la Oficina de Control Interno consultó los diferentes mapas de riesgos de seguridad de la información de cada uno de los procesos de la entidad registrados en el Sistema de Información de Procesos Automáticos SIPA, a su vez la política de gestión de activos de información (A-LE-474), Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (A-LE-505), la Guía para la Gestión de Activos de Información de la SDP (A-IN-016), y el registro de activos de información RAI (A-LE-283).

Se verificó cada uno de los documentos y actos que a continuación se relacionan teniendo en cuenta el código, la fecha de actualización y el número de acta para cada proceso así:

Tabla N. 12. Actualización Mapas de Riesgos de Seguridad de la Información

	PROCESO	CODIGO	FECHA	ACTA #
1	Administración de Recursos Físicos y Servicios Generales	A-LE-525	28/02/2024	112
2	Administración del Talento Humano	A-LE-518	26/02/2024	109
3	Contratación de Bienes y Servicios	A-LE-529	30/04/2024	182
4	Control Interno Disciplinario	S-LE-058	14/02/2024	92
5	Coordinación de Políticas Públicas y de Instrumentos de Planeación	M-LE-223	16/04/2024	178
6	Direccionamiento Estratégico	E-LE-103	15/02/2024	95
7	Evaluación y Control	S-LE-059	13/02/2024	91
8	Gestión de Recursos Financieros	A-LE-516	30/01/2024	46
9	Gestión Documental	A-LE-524	4/03/2024	120
10	Mejoramiento Continuo	S-LE-061	16/02/2024	96
11	Participación y Comunicación	E-LE-105	14/03/2024	172
12	Planeación Territorial y Gestión de sus Instrumentos	M-LE-224	14/02/2024	93

	PROCESO	CODIGO	FECHA	ACTA #
13	Producción, Análisis y Divulgación de la Información	M-LE-220	22/02/2024	108
14	Soporte Legal	A-LE-526	21/02/2024	106
15	Soporte Tecnológico	A-LE-521	5/02/2024	74

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

En la siguiente tabla se puede evidenciar que, de 109 controles identificados en los diferentes procesos de la Secretaría Distrital de Planeación para los riesgos de seguridad de la información, los de mayor participación son los procesos de Gestión Documental y Soporte Tecnológico cada uno con el 20% del total de los controles.

Tabla N. 13. Identificación riesgos y controles de Seguridad de la Información por proceso

PROCESO		RIESGOS	CONTROLES
1	Administración de Recursos Físicos y Servicios Generales	1	3
2	Administración del Talento Humano	2	8
3	Contratación de Bienes y Servicios	1	6
4	Control Interno Disciplinario	1	4
5	Coordinación de Políticas Públicas y de Instrumentos de Planeación	2	4
6	Direccionamiento Estratégico	2	5
7	Evaluación y Control	1	2
8	Gestión de Recursos Financieros	1	2
9	Gestión Documental	6	21
10	Mejoramiento Continuo	2	5
11	Participación y Comunicación	2	9
12	Planeación Territorial y Gestión de sus Instrumentos	1	4
13	Producción, Análisis y Divulgación de la Información	4	9
14	Soporte Legal	1	3
15	Soporte Tecnológico	5	24
TOTALES		**32**	**109**

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Con el fin de verificar los riesgos y los controles identificados en los diferentes mapas de Riesgos de seguridad de la información se tomaron como base los lineamientos señalados en la política de administración de riesgos E-LE-030 en el numeral 6.3 administración de riesgos de la información que establece: "*La gestión de riesgos de seguridad de la información, incluido su tratamiento, será aplicado sobre todos los activos de información de la SDP identificados por cada uno de los procesos y que hacen parte del Registro de Activos de Información de la SDP (RAI) – Tipo Software, Hardware. Redes y comunicaciones, infraestructura física, servicios, , Datos e información y personas que sean identificados con una criticidad ALTA, con base en lo establecido en la Guía para la Gestión de Activos de información de la SDP A-IN-016 y demás documentos para la administración del riesgo que hacen parte del Sistema de Gestión, las normas vigentes, la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5, el Anexo 4 – Lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas y las pautas y recomendaciones previstas en la NTC-ISO/IEC 27001".*

De acuerdo con lo señalado en el numeral 4 del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (A-LE-505) para la vigencia 2024, la actualización de instrumentos, de activos de información, aprobación de activos de información y publicación de los instrumentos (registros de activos de información e índice de información clasificada y reservadas) se tenía prevista entre febrero y abril de 2024. Sin embargo, la Oficina de Control Interno verificó que el documento Registro de Activos de Información (RAI) (A-LE-283) presenta en el SIPA su versión 11 de octubre de 2022, sin evidenciar la actualización de que trata el A-LE-505. Dado lo anterior, se recomienda establecer las acciones que permitan cumplir con lo programado y generar una versión actualizada de los activos de información acorde con la realidad de la entidad.

Igualmente, verificar y actualizar dichos activos de información y su nivel de clasificación o criticidad resultado de la valoración realizada de la Confidencialidad, Disponibilidad e Integridad, según la metodología y los lineamientos establecidos por el MinTIC en su Guía 5 *"Guía para la Gestión y Clasificación de Activos de información: seguridad y privacidad de la información",* y lo establecido en la Política de administración de riesgos E-LE-030 en el numeral 6.3 administración de riesgos de la información y a su vez con lo señalado en el numeral 4.7 Manejo de activos de la Política de gestión de activos A-LE-474 *"aplicando el modelo institucional de gestión de riesgos para identificar y tratar los riesgos que puedan afectar a los activos de información, que hagan parte del inventario de activos de información a su cargo y se encuentren clasificados en nivel de criticidad ALTA".*

Por otra parte, la Secretaría Distrital de Planeación identificó sus riesgos de seguridad con la siguiente tipología, definiendo la mayor cantidad de riesgos enfocados a la disponibilidad:

Tabla N. 14. Evaluación del Riesgo de Seguridad de la Información SDP

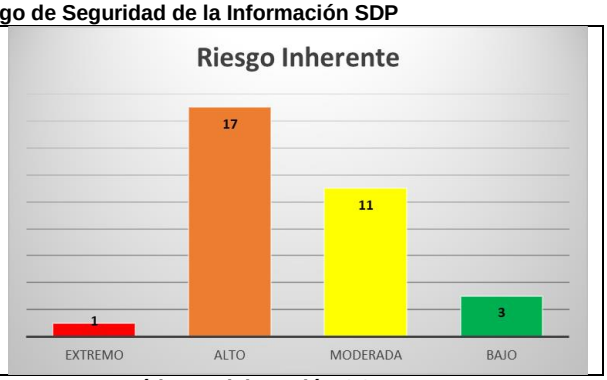
Tipo de Riesgo de Seguridad	CANTIDAD	%
Pérdida de Integridad	9	28%
Perdida de Disponibilidad	15	47%
Perdida de Confidencialidad	8	25%
Total	32	100%

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

En cuanto a su evaluación (Inherente vs Residual), la siguiente tabla registra los riesgos inherentes, donde 17 riesgos presenta calificación alta representando un 53% del total de riesgos, seguidos de los riesgos moderados con 11 riesgos correspondientes al 34%, 3 riesgos bajos y un riesgo extremo:

Tabla N. 15. Evaluación del Riesgo de Seguridad de la Información SDP

Perfil de Riesgos de Seguridad SDP		
Inherente	**TOTAL**	**%**
Extremo	1	3%
Alto	17	53%
Moderada	11	34%
Bajo	3	9%
TOTAL	**32**	**100%**



Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

En el seguimiento, no fue posible establecer o comparar el riesgo residual con el riesgo inherente, ya que no se observa una *Evaluación del Riesgo - Nivel del Riesgo Residual* unificada por cada riesgo, dado que se determina es por cada control. Por lo anterior, se recomienda la revisión de estos mapas de riesgos, a fin de que el método de valoración del riesgo Inherente (por riesgo o por combinación amenaza – vulnerabilidad) metodológicamente corresponda de igual manera al riesgo residual con promedio ponderado tomando todos los controles, en donde se evidencie el desplazamiento que tendrá el riesgo al evaluar el diseño de los controles.

Tabla 4. Riesgo Inherente Seguridad de la Información SDP

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

A su vez, la gestión de riesgos de seguridad de la información, incluido su tratamiento, identificados en cada uno de los procesos y que hacen parte del Registro de Activos de Información de la Secretaría Distrital de Planeación se encuentran clasificados como se muestra a continuación:

Tabla 5. Tipo de Activos del Riesgo de Seguridad de la Información SDP

TIPO DE ACTIVOS	CANTIDAD	%
Datos_Información	19	59%
Software	8	25%
Hardware	3	9%
Personas	1	3%
Infraestructura	1	3%
TOTAL	**32**	**100%**

Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Para los 32 riesgos identificados de seguridad de la información se registran 19 por datos_Información, que corresponde al 59% del total de activos identificados, que en primera instancia corresponden con los registros relacionados en cada uno de los procedimientos de la entidad. Por ejemplo: expedientes, las bases de datos, archivos de datos, contratos, acuerdos, documentos que soportan la gestión de la entidad, información sobre investigaciones, manuales internos y de gestión, procedimientos, guías y protocolos, cartografía física y digital, planes para la continuidad del negocio, acuerdos de recuperación y registros de auditoría, entre otros, seguidos por Software con 8 activos identificados correspondiente al 25% y Hardware con 3 correspondiente al 3%.

En cuanto a los controles a los Riesgos de Seguridad de Información, la siguiente tabla muestra la clasificación de los 109 controles identificados en los mapas de riesgos de seguridad de la información para cada uno de los procesos de la entidad, según atributos de eficiencia. Se puede evidenciar que 76 son Preventivos que corresponde al 70% del total de controles y cuyo fin es atacar la probabilidad de ocurrencia y se ejecutan ***antes*** de realizar la actividad originadora del riesgo, por otra parte se han identificado 13 controles Detectivos correspondientes al 12% y cuyo fin es atacar la probabilidad de ocurrencia del riesgo, y se activan ***durante*** la ejecución del proceso, y finalmente se presentan 20 controles correctivos con un 18% del total de los controles y cuyo fin es atacar el impacto frente a la materialización del riesgo y se ejecutan ***después*** de identificarlos.

Tabla 6. Valoración de los controles del Riesgo de Seguridad de la Información SDP

			Atributos de Eficiencia Controles			
Procesos		**Cantidad**	**Preventivo**	**Detectivo**	**Correctivo**	**Implementación**
1	Administración de Recursos Físicos y Servicios Generales	3	3	0	0	3 Manuales
2	Administración del Talento Humano	8	4	0	4	8 Manuales
3	Contratación de Bienes y Servicios	6	5	0	1	6 Manuales ,1 Automático
4	Control Interno Disciplinario	4	2	1	1	3 Manuales ,1 Automático
5	Coordinación de Políticas Públicas y de Instrumentos de Planeación	4	2	2	0	4 Manuales
6	Direccionamiento Estratégico	5	3	1	1	5 Manuales
7	Evaluación y Control	2	1	1	0	2 Manuales
8	Gestión de Recursos Financieros	2	2	0	0	2 Manuales
9	Gestión Documental	21	20	1	0	21 Manuales
10	Mejoramiento Continuo	5	4	0	1	4 Manuales ,1 Automático
11	Participación y Comunicación	9	4	1	4	6 Manuales ,3 Automático
12	Planeación Territorial y Gestión de sus Instrumentos	4	1	2	1	3 Manuales ,1 Automático
13	Producción, Análisis y Divulgación de la Información	9	6	0	3	3 Manuales , 6 Automáticos
14	Soporte Legal	3	3	0	0	3 automáticos
15	Soporte Tecnológico	24	16	4	4	23 Manuales , 1 Automático
	TOTALES	**109**	**76**	**13**	**20**	

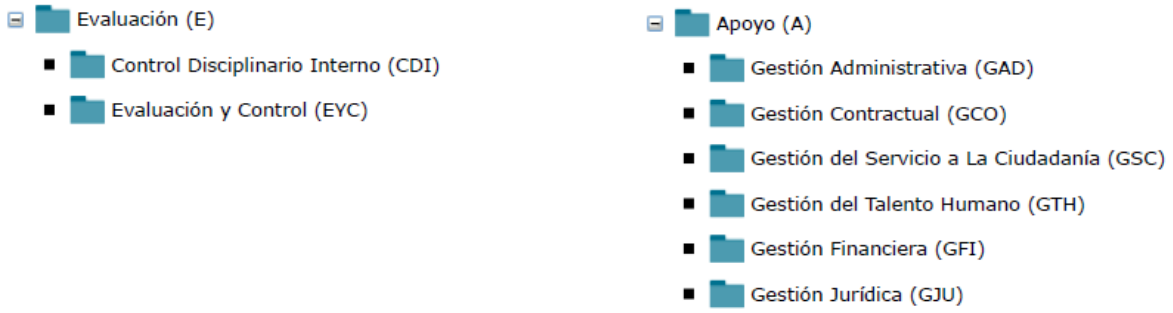
Fuente: Sistema de Información de Procesos Automáticos. Elaboración OCI.

Por otra parte, se evidencia que el 87% de estos controles (95) se realiza de forma Manual es decir ejecutados por personas y el 13% (14) son automáticos.

4.3 Evaluación Gestión Integral de Riesgos

A continuación, se presenta el análisis de los mapas de riesgos de gestión, corrupción y seguridad de la información por proceso, adicionalmente para los riesgos ambientales, del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT) vale aclarar que se toman desde el nombre anterior que se registra en SIPA, incluyendo en el análisis la nueva denominación. Al respecto, la Dirección de Planeación Institucional, señaló que *"Los nombres de las dependencias de conformidad con la última estructura organizacional de la entidad adoptada mediante Decreto 432 de 2022 se reflejan en los mapas de riesgos de cada proceso, pero asociados a los procesos que se encuentran parametrizados en el sistema SIPA, el cual por su forma de operar internamente dificultaba la parametrización de los nuevos procesos. Por tal razón, en la nueva herramienta tecnológica para el Sistema de Gestión "Gestiónate – Isolucion" si se verán reflejados los mapas de riesgos bajo la estructura del nuevo mapa de procesos."*. Por lo que en el nuevo aplicativo se reflejarán de la siguiente forma:

Gráfica N. 1. Nuevos Procesos SDP



Fuente: Respuesta a pregunta 5 cuestionario

Dentro de la evaluación se incluyeron también los riesgos ambientales, Sistema de Seguridad y Salud en el Trabajo (SSST) y Sistema de Administración del Riesgo de Lavado de Activos y Financiación al Terrorismo (SARLAFT).

Respecto a la materialización de riesgos, la *Política de Administración del Riesgo* E-LE-030 señala dentro de las responsabilidades de la primera línea de defensa *"Reportar los riesgos materializados en los objetivos, programas, proyectos, planes y actividades de los procesos que lideran."* y *"Definir los planes de acción para la mitigación de los riesgos materializados en cada uno de sus procesos."*. Sin embargo, del siguiente análisis se observaron una serie de eventos que se pueden considerar como materialización de riesgos, sin que hayan sido informado por la primera línea de defensa. Por lo anterior, la Oficina de Control Interno recomienda fortalecer la conceptualización y cultura de gestión del riesgo en lo relacionado con la materialización del riesgo y su tratamiento en la entidad, a fin de ponerlo en práctica en la realidad donde se desarrollan los diferentes procesos de la entidad.

4.3.1 Proceso Administración de Recursos Físicos y de Servicios Generales A-CA-004

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Dirección Administrativa - Subsecretaría Institucional
Nuevo Proceso	A-CA-012 Gestión Administrativa
Objetivo Proceso	Administrar los recursos físicos de la SDP, mediante la prestación de servicios logísticos, control de inventarios, adecuación de instalaciones y aseguramiento de bienes, para garantizar la continua operación de la entidad.

Tipo de Riesgo	Gestión
Riesgos	Posibilidad de afectación económica y reputacional por desmejoramiento de las buenas prácticas ambientales en la entidad y preservación del ambiente.
Causas	Incumplimiento de requisitos legales y ambientales, baja apropiación en la implementación de hábitos sostenibles por parte de los servidores y colaboradores para contribuir con la reducción en los impactos negativos al ambiente, generados por las actividades inherentes al funcionamiento de la Entidad.
Riesgos	Posibilidad de afectación económica y reputacional por disminución de la capacidad técnica y operativa de la secretaría distrital de planeación en la prestación de servicios de mantenimiento locativo y parque automotor,

Causas	Incremento en el nivel de deterioro de la Infraestructura física y parque automotor, solicitudes de mantenimiento locativo y transporte realizadas fuera de tiempo y sin los requisitos establecidos
Riesgos	Posibilidad de afectación económica por multas y sanciones de los entes reguladores.
Causas	inconvenientes con la supervisión en la ejecución de los contratos de apoyo logístico, bajo nivel de apropiación de lineamientos del Manual de Supervisión y de la normatividad legal vigente aplicable

Conclusiones: Se recomienda tener en cuenta los hallazgos administrativos contemplados en los planes de Mejoramiento "*3.2.2.1 Hallazgo administrativo con presunta incidencia disciplinaria por diferencia en los datos reportados en la plataforma SIVICOF en el reporte CBN 1111 4 y los datos entregados por la SDP correspondiente al PRESUPUESTO EJECUTADO PARA LA META / ACCIÓN AMBIENTAL EN LA VIGENCIA FISCAL del factor gestión ambiental PACA vigencia 2022*". así como la identificación de nuevos riesgos y asociarlos al cumplimiento de requisitos legales y ambientales, a su vez actividades de promoción y sensibilización en temas ambientales para el cuidado de los recursos naturales y del medio ambiente para la SDP.

Por otra parte, se recomienda ampliar la identificación de riesgos contemplando la posibilidad de pérdida o daño de los bienes de la entidad por daños atribuibles a personas ajenas a la entidad o hechos accidentales, al manejo de los inventarios ya sea por traslados, dados de baja o suministro de insumos y a la perdida de garantía de dichos bienes.

Tipo de Riesgo	**Corrupción**
Riesgos	Posibilidad de manejo indebido de la información relacionada con el proceso y/o abuso del poder, con el fin de interferir en la gestión para beneficio propio o de un tercero.
Causas	1. Registro erróneo de forma intencional en los sistemas de información para beneficio propio o de un tercero. 2. Omisión o incumplimiento de procedimientos para agilizar una actividad propia del proceso.

Conclusiones: Se recomienda fortalecer las causas y controles teniendo en cuenta que estas acciones aumentan la probabilidad de manipular los datos generando vulnerabilidades que pueden comprometer la integralidad y confidencialidad de la información, a su vez fortalecer el plan de acción para el tratamiento del riesgo ya que se relaciona *"Socializar internamente a los servidores de la Dirección Administrativa a que haya lugar, los procedimientos, guías, instructivos, formatos y riesgos con el fin de fortalecer el conocimiento de la dependencia y sus actividades propias".* la cual no indica la fecha en que se realiza la sesión ni la cantidad de sesiones a realizar durante la vigencia 2024.

Tipo de Riesgo	**Seguridad de la Información**
Activo de Información	Datos Información Planes, programas, historias, inventarios
Riesgo	Posibilidad de Perdida de Integridad por agua; de planes, programas, historias, inventarios,
Causa	Debido a ausencia de copias de respaldo o backup de la información, ausencia de copias de respaldo o backup de la información
Objetivo de Control 1.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas

Control	El servidor público debe mantener actualizada la información a cargo para lo cual realizará copias de respaldo con la frecuencia establecida.
Objetivo de Control 2.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes
Control	La Dirección de Tecnologías y de la información y Comunicaciones socializa las directrices en Seguridad de la Información para su respectiva aplicación.
Objetivo de Control 3.	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
Control	El líder del proceso asegura que los equipos se encuentren en una ubicación adecuada y protegidos de las condiciones ambientales que los ponga en riesgo (fuego y agua).

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presenta niveles de criticidad medio y bajo, se sugiere evaluar y actualizar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo se debe gestionar dichos riesgos. Por otra parte, se sugiere analizar la causa del riesgo como la ausencia de copias de respaldo o backups de la información que verdaderamente sean las necesarias para mitigar dicho riesgo y sus consecuencias. Finalmente se sugiere revisar si existen riesgos de confidencialidad de la información ya sea Publica reservada o clasificada que puedan afectar el proceso.

En cuanto al objetivo de control y el control, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, detallar cómo se actúa en caso de que el control falle.

Igualmente, en la descripción de los controles no se evidencian la frecuencia o la periodicidad con la que se realiza o ejecuta la actividad. Finalmente, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación.

4.3.2 Proceso de Gestión del Talento Humano

Objetivo Estratégico	4. Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Dirección de Talento Humano
Proceso Anterior	Administración del Talento Humano A-CA-005
Objetivo Proceso	Proveer, potencializar y administrar el talento humano de la SDP a través de políticas, estrategias y acciones que contribuyan al cumplimiento de la nacionalidad de la entidad, así como el pleno desarrollo de los servidores.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por incumplimiento de la ejecución de los programas de bienestar, capacitación, seguridad y salud en el trabajo, debido a:
Causas	1. Inadecuada identificación de las necesidades de los planes y programas por parte de los procesos 2. Fuga de conocimiento por movimientos de personal 3. Cambios en la normatividad 4. Falta de participación en las actividades y/o situaciones fortuitas (eventos socio naturales), que no permitan realizar una adecuada gestión del talento humano.
Controles	1. El profesional universitario y/o especializado de Talento Humano responsable valida anualmente a través del resultado de la encuesta de necesidades, encuesta de percepción, resultados de los Planes de los años anteriores y sugerencias recibidas por diversos mecanismos que la formulación del Plan Institucional de Capacitación, el Plan de Bienestar y el Programa de Seguridad y Salud en el trabajo, contengan los insumos y lineamientos establecidos en la normatividad para su estructuración y envía correo electrónico con el documento preliminar al (la) director(a) del área para poner el anuncio para la actualización de cada plan y su publicación en la página web de la entidad una vez haya sido aprobado por el Comité Institucional de Gestión y Desempeño, según acta de reunión que lleva la Secretaria del Comité. 2. El profesional universitario y/o especializado de Talento Humano valida a través del archivo de diapositivas del Plan que anualmente se elabora, la presentación del proyecto de plan a la Comisión de Personal para su revisión y recomendaciones, lo cual queda registrado en las actas del comité que custodia la Dirección de Talento Humano como secretaria técnica del comité 3. El(la) Director(a) de Talento Humano verifica trimestralmente el cumplimiento del cronograma de actividades definidas en los planes y programas de la Dirección, a través del seguimiento al POA del proceso; cuando se evidencian retrasos en la ejecución, se reúne con el responsable, para analizar las causas y definir la acción a seguir, lo cual se evidencia en el reporte del POA del siguiente periodo. 4. El auxiliar administrativo, el profesional universitario y/o especializado y el Director de Talento Humano revisan cada vez que ingresa personal nuevo a la entidad, que se ejecute el procedimiento de Inducción y reinducción de personal (A-PD-008), se aplique el Manual de Inducción (A-IN019), se diligencie el Formato de Inducción en el Puesto de Trabajo (AFO-205), se incluya en la historia laboral del servidor nuevo y se programen las jornadas de inducción dentro de los cuatro (4) meses siguientes a la posesión; si no ha sido programado o no pudo asistir a alguna jornada se hace la programación o reprogramación según sea el caso, verificando que todo nuevo servidor tenga su certificado de asistencia o diploma de la Inducción Institucional en su historia laboral. 5. El profesional universitario y/o especializado de Talento Humano verifica cada vez que hay una solicitud de capacitación financiada por la entidad, que se radiquen por SIPA las cartas de compromiso (AFO- 109), que los obliga a transferir los conocimientos para mejorar la prestación del servicio en la Secretaría Distrital de Planeación, sirviendo de agente capacitador dentro o fuera de la Entidad, cuando el tema y la entidad así lo requieran, para lo cual debe remitir evidencia de la actividad realizada, dentro de los 2 meses siguientes a la finalización del curso, de no hacerlo, se le requerirá su ejecución 6. El profesional universitario y/o especializado Talento Humano responsable de formular las estrategias de intervención en clima laboral, revisa que en el Plan de Bienestar Social la respectiva vigencia, se incluya un ítem referido a la intervención y dichas acciones sean incluidas en el POA de la vigencia. 7. El profesional universitario y/o especializado y el(la) Director(a) de Talento Humano revisan trimestralmente a través de los informes de seguimiento que se hacen, que las

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por incumplimiento de la ejecución de los programas de bienestar, capacitación, seguridad y salud en el trabajo, debido a:
	actividades que quedaron definidas o aprobadas en los diferentes planes, se estén ejecutando, así como su estado de avance, lo cual debe quedar soportado en el repositorio de evidencias y registrado en el POA de la vigencia. 8. El profesional universitario y/o especializado y el(la) Director(a) de Talento Humano verifican el cumplimiento del cronograma de actividades definidas en la estrategia a través del seguimiento al POA del proceso que se hace trimestralmente, a fin de corroborar posibles retrasos en la ejecución, en cuyo caso se reúne con el responsable para analizar las causas y definir la acción a seguir, lo cual queda soportado con las evidencias en el repositorio y el reporte del siguiente periodo 9. El profesional universitario y/o especializado y el(la) Director(a) de Talento Humano verifican, una vez finalizada la estrategia de intervención, que se registre en el POA de la siguiente vigencia, la medición del clima laboral

Conclusiones: Se establecen 4 causas raíz. Se recomienda ajustar la redacción de las causas, dado que al final se señala *"que no permiten realizar una adecuada gestión del talento humano"*, lo que se asemeja más a una consecuencia que a una causa. Por otra parte, se establecen 9 controles para el riesgo, por lo que se sugiere priorizarlos a fin de establecer aquellos que efectivamente ataquen las principales causas definidas. Lo anterior, en búsqueda de la optimización en la gestión del riesgo. En cuanto a la evaluación del riesgo, se sugiere prestar especial atención al impacto en lo referente al tema de Seguridad y Salud en el Trabajo, dada la obligatoriedad normativa que regula el tema.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por acciones judiciales y/o pérdida de credibilidad, debido a:
Causas	1. Errores o inconsistencias en la liquidación de la nómina, 2. Flexibilización en los tiempos establecidos para radicar las novedades del mes, 3. Recepción de novedades por canales diferentes al establecido (SIPA) y 4. Debilidad en la cultura institucional para atender y cumplir las circulares emitidas por la Dirección de Talento Humano

Conclusiones: Se sugiere la revisión de las causas raíz definidas, atendiendo a que las causas 2 y 3 se pueden entender como consecuencia de la causa 4 Debilidad en la cultura institucional para atender y cumplir las circulares emitidas por la Dirección de Talento Humano.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación reputacional por pérdida o extravío de las historias laborales o de los documentos que reposan en las mismas, debido a insuficiencia de recursos tecnológicos apropiados para el adecuado desarrollo de las actividades archivísticas, inadecuada aplicación de las normas, procesos y procedimientos que generan demandas o investigaciones y recursos económicos limitados para desarrollar los planes a cargo del proceso
Causas	1. Insuficiencia de recursos tecnológicos apropiados para el adecuado desarrollo de las actividades archivísticas,

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación reputacional por pérdida o extravío de las historias laborales o de los documentos que reposan en las mismas, debido a insuficiencia de recursos tecnológicos apropiados para el adecuado desarrollo de las actividades archivísticas, inadecuada aplicación de las normas, procesos y procedimientos que generan demandas o investigaciones y recursos económicos limitados para desarrollar los planes a cargo del proceso
	2. Inadecuada aplicación de las normas, procesos y procedimientos que generan demandas o investigaciones y 3. Recursos económicos limitados para desarrollar los planes a cargo del proceso
Controles	1. El auxiliar administrativo a cargo de historias laborales de Talento Humano mensualmente verifica por correo electrónico que los documentos de las transferencias documentales internas que se hacen al archivo de Historias Laborales, cumplan con lo establecido en el Reglamento de Archivo A-IN 434 a fin de corroborar la información recibida e informar a través de correo al responsable las novedades. 2. El auxiliar administrativo a cargo de historias laborales de Talento Humano verifica cada vez que se requiera, que el formato -Hoja de Control expediente de archivo (A-FO- 387) esté actualizado conforme con la documentación que reposa en las historias laborales. En caso de encontrar alguna novedad, procede a solicitar los ajustes correspondientes. 3. El auxiliar administrativo de Talento Humano verifica diariamente o cuando hay documentos radicados en SIPA, la correspondencia (Reparto) con destino a Historias Laborales a fin de corroborar que sean registrados en el AFO- 058 formato único de inventario documental para relacionar todos los documentos que ingresan a la oficina para ser archivados. 4. El auxiliar administrativo a cargo de historias laborales de Talento Humano cada vez que haya solicitudes de consulta de historias laborales verifica que esté diligenciado el A-FO-357 «Control préstamo de Historias Laborales» en cumplimiento del reglamento de Archivo(A-IN-434), o que la consulta digital haya quedado registrada en el control de atención telefónica, a fin de corroborar quién tiene el expediente laboral en caso de alguna novedad. 5. El auxiliar administrativo de Talento Humano revisa cada vez que hay inspecciones, que no haya saturación de documentos, y que se cumpla con las condiciones de temperatura, humedad y luz adecuados para albergar las historias laborales conforme con lo establecido en el reglamento de Archivo(A-IN-434); en caso de incumplimiento, corrobora que se haya puesto la incidencia por mesa de ayuda para la adecuación del espacio físico. 6. El auxiliar administrativo de Talento Humano cada que elabora el diagnóstico para intervenir los expedientes laborales de personas que hayan demandado verifica que la información de la base de datos esté actualizada conforme con los lineamientos del reglamento de Archivo(A-IN-434) y corrobora que ésta repose en el archivo de historias laborales y sea entregada a la Dirección de Talento Humano. 7. El auxiliar administrativo de Talento Humano cada vez que haya personal nuevo en el área que tenga dentro de sus obligaciones las del archivo de historias laborales, verifica que se le haya socializado el Reglamento de Archivo para la conformación y organización documental de historias laborales y quede registrado en el formato A FO 205-inducción en el puesto de trabajo y corrobora que quede constancia en el formato de control de reuniones (A-FO 184).

Conclusiones: Dado que corresponde a un riesgo asociado a la disponibilidad e integridad de un activo de información, se sugiere que sea unificado con el riesgo 4 y que haga parte del A-LE-518 *Mapa de Riesgos de Seguridad de la Información del Proceso Administración del Talento Humano*. Igualmente, se recomienda ajustar la redacción de las causas raíz, dado que la causa 2 incluye

una consecuencia *"que generan demandas o investigaciones"*. Por otra parte, se establecen 7 controles para el riesgo, por lo que se propone su revisión dado que no fue posible establecer relación directa entre las causas y los controles, además todos se establecen bajo la responsabilidad del auxiliar administrativo. Adicionalmente, se recomienda su priorización a fin de establecer aquellos controles que efectivamente ataquen las principales causas definidas, minimizando la materialización del riesgo. En cuanto a la evaluación del impacto del riesgo se considera importante tener en cuenta las consecuencias que puede tener la materialización del riesgo, lo que permitirá la definición de controles defectivos y/o correctivos. No es claro el control 6, dado que da a entender que se refiere a demandas, de ser así se sugiere un control más robusto que ataque el impacto frente a la materialización del riesgo.

Tipo de Riesgo	**Información**
Activo de Información	**Datos Información. Historias laborales**
Riesgo	Posibilidad de pérdida de confidencialidad por:
Causas	1. Fallas humanas 2. Divulgación ilegal de la información de las historias laborales 3. Manejo manual de la información y copias no controladas
Objetivo de Control	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Control	Cada vez que se vinculan servidores o servidoras al proceso A-CA-005 están en la obligación de asistir y participar activamente en las capacitaciones que sean programadas por la entidad para lo cual deben diligenciar el formato A-FO-205 (Inducción en el puesto de trabajo) y el formato de asistencia (A-FO 183), según sea el caso.
Objetivo de Control	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
Control	Todos los servidores del proceso están en la obligación de guardar y verificar la información que gestiona diariamente en la carpeta compartida que la Dirección de Tecnologías de la Información y las Comunicaciones habilitó para tal fin y que queda registrado en la hoja de control (A-FO 258 Bitácora Solicitud Cuentas de Usuario); por lo tanto, no está autorizado realizar copias no contraladas en diferentes medios removibles

Conclusiones: Se sugiere su unificación con el riesgo 3, fortaleciéndolo con la inclusión del criterio de integridad del activo. Se recomienda establecer controles que ataquen directamente las causas raíz definidas, dado que la asistencia a capacitaciones desdibuja la realidad de un control que permita reducir o mitigar el riesgo, sin desconocer que pueden aportar a la mejora. Lo anterior, atendiendo a que se refiere a un activo con datos sensibles. En cuanto a la evaluación del impacto del riesgo, se considera importante tener en cuenta las consecuencias que puede tener la materialización del riesgo, lo que permitirá la definición de controles defectivos y/o correctivos. En cuanto al plan de acción, atendiendo a que se orienta únicamente a sensibilizaciones, se considera importante fortalecerlo para que permita la gestión de la posible pérdida de confidencialidad de la información almacenada en las historias laborales.

Tipo de Riesgo	Información
Activo de Información	Datos Información. Los registros e información que se generan o se ingresan con ocasión de las actividades (Nómina, Seguridad Social, Capacitación, Bienestar, Seguridad y Salud en el Trabajo, EDL) a cargo de la Dirección
Riesgo	Posibilidad de pérdida de disponibilidad por:
Causas	1. Mal funcionamiento del software 2. Fallas del equipo 3. Fallas humanas 4. Error en el uso o abuso de derechos y privilegios 5. Falsificación de derechos de acceso 6. Retraso en la salida de información de los sistemas 7. Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información 8. Errores u omisiones en el registro de los datos e información que se gestiona diariamente.
Objetivo de control	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control	El profesional Universitario o Especializado de la Dirección de Tecnologías de la Información y las Comunicaciones revisa que se cumpla con el cronograma de realización de las copias de seguridad en la carpeta compartida de cada dependencia oportunamente y genera capacitaciones para que los servidores soliciten por la mesa de ayuda las correspondientes copias de respaldo de sus equipos de cómputo dando cumplimiento a la periodicidad indicada en la Política de Seguridad de la Información y demás documentos concordantes
Objetivo de control	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
Control	El profesional especializado responsable en la Dirección de Talento Humano registra en SIPA los proyectos de actos administrativos para que se generen los documentos definitivos a fin de controlar que queden registrados en el repositorio de SIPA para asegurar el producto de salida
Objetivo de control	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
Control	El director o encargado de la Dirección de Talento Humano solicita mediante el diligenciamiento del formato A-FO-227 Solicitud requerimiento usuario (sistemas de información/aplicaciones de software) y la creación de requerimientos a través del Sistema de Requerimientos, el desarrollo de aplicaciones o módulos para registrar información de actividades que ejecuta la Dirección, lo cual se controla mediante el número del requerimiento que genera el aplicativo hasta que se ponga en producción lo solicitado.
Objetivo de control	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
Objetivo de control	El superior inmediato de cada área verifica cada vez que haya un ingreso o un retiro de personal a través de la creación de una incidencia en la Mesa de Ayuda que se soliciten o eliminen los accesos a los sistemas de información mediante el diligenciamiento del formato A-FO-010 y para los retirados reporta en el formato A-FO-128 el número de la incidencia que arrojó el aplicativo de la Mesa de Ayuda, con lo cual se controla que solo personal autorizado tenga acceso a información que maneja el área.
Control	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
Objetivo de control	El superior inmediato de cada área verifica cada vez que haya un ingreso o un retiro de personal a través de la creación de una incidencia en la Mesa de Ayuda que se soliciten

Tipo de Riesgo	Información
Activo de Información	Datos Información. Los registros e información que se generan o se ingresan con ocasión de las actividades (Nómina, Seguridad Social, Capacitación, Bienestar, Seguridad y Salud en el Trabajo, EDL) a cargo de la Dirección
Riesgo	Posibilidad de pérdida de disponibilidad por:
	o eliminen los accesos a los sistemas de información de acceso privilegiado mediante el diligenciamiento del formato A-FO-010 y para los retirados reporta en el A-FO-128 el número de la incidencia que arrojó el aplicativo de la Mesa de Ayuda, con lo cual se controla que solo personal autorizado tenga acceso a información que maneja el área.
Control	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Objetivo de control	El profesional Universitario o Especializado de la Dirección de Tecnologías de la Información y las Comunicaciones cada vez que haya una actualización o generación de una nueva directriz debe revisar y garantizar que se actualice en SIPA el conjunto de políticas para la seguridad de la información una vez sea aprobada por el Comité Institucional de Gestión y Desempeño y una vez esté versionada en el aplicativo SIPA y solicita mediante correo electrónico o comunicación a la Oficina de Comunicaciones que la publique y comunique a los empleados y a las partes externas pertinentes y también que se incluya el nuevo contenido en las jornadas de inducción que hace la DTIC programadas por la Dirección de Talento Humano y en el programa de capacitaciones de la DTIC

Conclusiones: No fue posible identificar en el documento A-LE-283 *Registro de Activos de Información (RAI)*, el activo definido para este riesgo, además que, para el caso de este proceso, solo se relaciona un activo con nivel de criticidad ALTO correspondiente a historias laborales. Por lo anterior, se sugiere evaluar la criticidad de los activos de información del proceso, a fin de determinar si corresponde a un nivel ALTO a fin de aplicar la gestión de riesgos, según lo establecido en la *Guía para la Gestión de Activos de Información* (A-IN-016) y la *Política de Administración del Riesgo* (E-LE-030). Además, tener en cuenta que la información a la que se refiere puede corresponder a datos sensibles de información de los funcionarios y exfuncionarios y por otro la redacción del activo de información menciona aplicativos pertenecientes a otras entidades (EDL, ARL).

En cuanto a las causas raíz definidas, de la redacción del riesgo se pueden extraer 8, por lo que se sugiere la revisión de la redacción del riesgo priorizando las principales causas. Referente a los controles, se establecen 6 para su tratamiento, por lo que se considera necesario su priorización a fin de establecer aquellos que efectivamente ataquen las principales causas que generan el riesgo. Adicionalmente, los controles 4 y 5 se registran bajo la responsabilidad del *"superior inmediato de cada área"* por lo que se sugiere su revisión a fin de establecer a la Dirección de Talento Humano como responsable, porque puede dar a entender que para el caso de este riesgo específico el control se debe aplicar a todas las áreas.

Por otra parte, se recomienda la revisión del A-LE-518 *Mapa de Riesgos de Seguridad de la Información del Proceso Administración del Talento Humano,* a fin de que muestre la *Evaluación del Riesgo - Nivel del Riesgo Residual* por riesgo y no por cada control como está apareciendo actualmente. Atender lo indicado en el *Informe de Auditoría de Sistemas de Gestión* de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

Adicionalmente, para los riesgos de seguridad de la información se requiere la revisión de aquellos controles catalogados como correctivos, atendiendo su definición en la política de administración del riesgo E-LE-030 *"ataca el impacto cuando el riesgo ya se ha materializado. El control se acciona posterior a la ejecución del proceso o actividad y ya se han presentado las consecuencias.".*

Tipo de Riesgo	Corrupción
Riesgo	Manipulación dolosa de los registros y/o documentos de los procedimientos a cargo de la Dirección de Talento Humano para favorecer los intereses propios o de terceros
Causas	1. Recursos económicos limitados para desarrollar los planes a cargo del proceso, 2. Ausencia de una aplicación confiable para la administración de las historias laborales, 2. Contratación de personal con poco conocimiento para adelantar actividades de Actualización de la información, 3. Deficiente aplicación de normas archivísticas impacta en la gestión del proceso lo cual genera demandas o investigaciones
Controles	1. El Profesional Universitario o Especializado de Seguridad de la información de la Base de datos de la Dirección de Tecnologías de la Información y las Comunicaciones, verifica cada vez que haya un retiro a través del formato A-FO-010 que se haya restringido el acceso a los aplicativos PERNO, EDL, CETIL, etc., a personal no autorizado por la Dirección de Talento Humano para evitar accesos prohibidos y únicamente son autorizados los que autoriza el director de Talento Humano a través de la mesa de ayuda adjuntando el formato A-FO-010 con datos del servidor/contratista información que . El auxiliar de DTH verifica cuando el personal retirado remita radicado por SIPA el formato A-FO-128 con el número de la incidencia en la casilla correspondiente para la eliminación de accesos a los aplicativos, en caso de que no esté registrado este dato el auxiliar devolverá el formato hasta que se subsane esta inconsistencia. 2. El auxiliar administrativo de Talento Humano verifica cada vez que haga un nuevo ingreso o encargo, a través de comunicación dirigida al jefe de cada dependencia que diligencie el Formato de Inducción en el puesto de trabajo A-FO-205 para que se divulguen los procedimientos y controles, haciendo mención de la obligatoriedad de la aplicación de los aspectos funcionales actividad 5 del Formato en mención, en relación con las responsabilidades del cargo y si amerita, reitera comunicación a los jefes para recordarles la obligatoriedad de la actividad, cada vez que haya una jornada de inducción. 3. El subsecretario/jefe/director/subdirector inmediato de cada área verifica cada vez que haya un ingreso o un retiro de personal a través de la creación de una incidencia en la Mesa de Ayuda que se soliciten o eliminen los accesos a los sistemas de información mediante el diligenciamiento del formato A-FO-010 y para los retirados reporta en el A-FO-128 el número de la incidencia que arrojó el aplicativo de la Mesa de Ayuda, con lo cual se controla que solo personal autorizado tenga acceso a información que maneja el área. 4. El auxiliar administrativo de Talento Humano cada vez que haya un ingreso o aporte de diplomas de estudio verifica por medio de correo electrónico o por comunicación radicada en SIPA que se haya solicitado a las instituciones educativas la validez de las certificaciones de estudio formal aportadas por los servidores que se vincularon en un cargo y si es del caso, procede conforme lo establece la ley, copia de ésta comunicación se remite mediante transferencia documental interna por correo electrónico con la respuesta de la institución educativa al archivo de Historias laborales para que repose en la historia laboral del aportante o nuevo servidor. 5. El profesional Universitario o Especializado de la Talento Humano verifica cada vez que vez que haya un postulante a un cargo vacante, a través del A-FO-245 que se apliquen

Tipo de Riesgo	Corrupción
Riesgo	Manipulación dolosa de los registros y/o documentos de los procedimientos a cargo de la Dirección de Talento Humano para favorecer los intereses propios o de terceros
	los controles de las actividades 2 y 4 del procedimiento A-PD-005 Vinculación de personal, relacionadas con la identificación de la modalidad o carácter de vinculación, revisando que cumpla con los requisitos de experiencia, estudios y conocimientos básicos esenciales a fin de que se establezca su conformidad con el Manual de Funciones y en caso de que no se diligencie el formato se devuelven los documentos aportados hasta que sea diligenciado el A-FO-245, información que se remite mediante transferencia documental interna por correo electrónico con los anexos al Archivo de Historias laborales para que repose en la historia laboral del postulante o nuevo servidor. 6. El auxiliar administrativo de Talento Humano verifica cada vez que haya una solicitud de certificación laboral de funciones a través de la certificación proyectada, que se aplique el Procedimiento de emisión de certificaciones (A-PD-022) Actividad 9 revisando que la certificación contenga lo establecido en la historia laboral del (la) solicitante, lo cual es validado posteriormente con la revisión y firma del director de Talento Humano.

Conclusiones: Se recomienda la revisión de la redacción del riesgo, ya que generaliza la actuación del proceso, de tal forma que no es posible identificar claramente a qué se refiere (vinculación, manejo de información, contratación, entre otros), lo que se comprueba con las 3 causas definidas relacionadas con temas diferentes que gestiona el área, lo que puede dificultar la calificación de los *Criterios de impacto para riesgos de corrupción*. Adicionalmente, dentro de las causas se señala *"lo cual genera demandas o investigaciones"* que puede corresponder más a una consecuencia que a una causa. Por otra parte, se sugiere priorizar los controles establecidos a fin de establecer aquellos que efectivamente ataquen las principales causas definidas.

En cuanto al contexto definido en el mapa de riesgos, se incluye el objetivo estratégico *"8.Desarrollar e implementar una estrategia de gestión del conocimiento e innovación interna que permita retener experiencias y fomentar nuevas formas de trabajo y soluciones innovadoras en la entidad además, de apoyar la formulación de la política de CTi en el Distrito."* sin que dentro de los riesgos definidos se haya identificado un riesgo directamente relacionado, más aún cuando la Dirección es una de las líderes de la política de Gestión del Conocimiento y la Innovación. Por lo anterior, se considera importante atender la recomendación dada por la Dirección de Planeación Institucional en su *Informe Monitoreo de Segunda Línea de Defensa a los Mapas de Riesgos de Gestión, Corrupción y de Seguridad de la Información de la Secretaría Distrital de Planeación* respecto a considerar la inclusión de riesgos asociados a Gestión del Conocimiento y la Innovación, en conjunto con la Dirección de Planeación Institucional, Oficina de Laboratorio de Ciudad y Dirección de Tecnologías de la Información y las Comunicaciones.

Por otra parte, se sugiere que, para la definición de los riesgos, se tengan en cuenta los planes de mejoramiento que se han generado al proceso y que actualmente corresponden a las siguientes 3 situaciones de mejora:

- 2176: Dentro del proceso de encargos, se evidencian incumplimientos de los funcionarios objeto de esta novedad administrativa, en cuanto a la formalización de la entrega del cargo, la capacitación en el puesto de trabajo y Teletrabajo.
- 2177: Novedades de registro público de carrera administrativa (incorporación y retiro) por fuera de los tiempos establecidos de la norma.

- 2178: No se supera la situación crítica consignada en el informe de seguimiento adelantado en mayo de 2022, dado que no fueron formuladas acciones correctivas por parte de la Dirección de Talento Humano que permitieran subsanar la causa raíz identificada (fueron formuladas dos correcciones), y es de tener en cuenta que en Acta 01 CNCS (Reuniones CNSC y SDP 23/05/2023, 24/05/2023 y 25/05/2023), la Comisión Nacional del Servicio Civil resalta la obligatoriedad que tiene la entidad de reportar la totalidad de la Oferta Pública de Empleos de Carrera de los empleos que se encuentren en vacancia definitiva, informando que la CNSC no acepta iniciar proceso de selección con OPEC parciales, y adicionalmente no se destinaron recursos presupuestales de manera oportuna (sólo hasta el mes de agosto de 2023) para cubrir este proceso de convocatoria.

4.3.3 PROCESO CONTRATACIÓN DE BIENES Y SERVICIOS A-CA-006

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Dirección de Gestión Contractual
Nuevo Proceso	A-CA-011 GESTIÓN CONTRACTUAL
Objetivo del Proceso	Adquirir productos, bienes y servicios de manera eficiente y transparente, a través de procesos de contratación adelantados dentro del marco que establece la normatividad vigente, con el fin de satisfacer necesidades que en materia contractual requieran las dependencias de la SDP, contribuyendo así al cumplimiento de los fines y objetivos institucionales.

Tipo de Riesgo	Gestión
Riesgos	Posibilidad de afectación económica y reputacional por inexactitud en la identificación y/o descripción de los requisitos técnicos, que no permitan satisfacer la necesidad de la entidad y/o la adquisición de bienes, productos o servicios no requeridos, que conlleven a sanciones del respectivo ente de control.,
Causas	Falencias en la estructuración de los documentos precontractuales (información y documentación incompleta)
Riesgos	Posibilidad de afectación económica y reputacional por no recepción de ofertas y/o imposibilidad para la selección de la oferta más favorable, generando reprocesos que impiden (i) la satisfacción de la necesidad evidenciada (ii) la correcta ejecución del plan anual de adquisiciones (iii) cumplimiento de metas institucionales.,
Causas	Solicitud de requisitos que no cumplen los oferentes del sector, desconocimiento o mal uso del SECOP II, por parte del oferente.
Riesgos	Posibilidad de afectación económica y reputacional por falencias en el ejercicio de la supervisión e interventoría debido a un deficiente seguimiento a obligaciones del contrato a cargo del contratista, que conlleven a la declaratoria de incumplimiento del contrato (parcial o total) y/o investigaciones del respectivo ente de control,
Causas	Desconocimiento de la rigurosidad de la función, falta de comunicación oportuna frente a los inconvenientes en la ejecución de los contratos y/o designación de supervisor que no cuenta con los conocimientos requeridos para ejercer la función, gran cantidad de contratos a vigilar-supervisar que sobrepasan la capacidad laboral del supervisor

Conclusiones: Se recomienda establecer nuevos riesgos o fortalecer los controles ya existentes conforme a los hallazgos administrativos contemplados en el Informe de Auditoría de Regularidad de la Contraloría de Bogotá con presunta incidencia fiscal y disciplinaria, por tomar el mayor valor del estudio de mercado, vulnerando el principio de eficiencia fiscal, a su vez por no realizar el

estudio de mercado para determinar los valores de los contratos y justificar que las entidades contratadas fueron las mejores ofertas de los servicios y productos requeridos por la administración, y finalmente por no requerir a un proponente cuando se evidencia precios artificialmente bajos, en el proceso de selección.

Por otra parte, en la descripción de los controles se debe puntualizar a que hace referencia tanto el equipo de trabajo de la dirección de contratación como en los integrantes del comité evaluador y cuál es el rol que ejerce en la ejecución del control, es importante establecer el cargo (profesional, técnico, coordinador o jefe).

A su vez se recomienda verificar y contemplar nuevos riesgos, causas y controles conforme a los hallazgos o situaciones críticas identificadas en el Informe Definitivo del Proceso de Contratación de Bienes y Servicios de la Secretaría de Planeación Distrital por la OCI así:

1. Debilidad en la justificación de la forma de Selección del Contratista, Estudio de sector, estudio de mercado y fijación de honorarios
2. Debilidad en los estudios previos de la contratación
3. Incumplimiento al Principio de Planeación que rige la contratación estatal
4. Fallos en la supervisión del contrato - seguimiento técnico, administrativo financiero y contable
5. Contratación por prestación de servicios, de actividades establecidas en las funciones de cargos descritos en el Manual de funciones de la entidad
6. Omisión en la Publicación de documentos en el SECOP II

Así mismo, se sugiere atender lo indicado en el Informe de Auditoría de Sistemas de Gestión de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos.".* Finalmente, en los controles identificados no se registra la evidencia de la ejecución del control y donde quedan almacenados dichos controles.

Tipo de Riesgo	**Corrupción**
Riesgos	Posibilidad de direccionamiento o ajuste de los estudios previos y demás documentos de las etapas de planeación y selección del proceso de contratación, en favor de un tercero, omitiendo el cumplimiento del principio de selección objetiva (Etapa Precontractual)
Causas	Estudios previos deficientes o manipulados para beneficiar a un proponente en particular
Riesgos	Posibilidad de ejercer la supervisión o interventoría de contratos de manea desleal o interés ilícito en su ejercicio a través de la manipulación y/o extralimitación y/u omisión de funciones en beneficio del contratista o de un tercero (Etapa Contractual - Postcontractual)
Causas	Deficiencia en el ejercicio de la supervisión y/o la interventoría (amiguismo)

Conclusiones: Si bien es cierto los riesgos y las causas están identificados para las etapas precontractual (estudios previos deficientes o manipulados para beneficiar a un proponente en particular) contractual y postcontractual (Deficiencia en el ejercicio de la supervisión y/o la interventoría (amiguismo)) es importante contemplar el manejo de ausencia o debilidad de medidas y/o políticas de conflictos de interés, adendas que cambian condiciones generales del proceso para favorecer a grupos determinados, otorgar labores de supervisión a personal sin conocimiento para ello.

Tipo de Riesgo	**Seguridad de la Información**
Tipo de Activo	Datos Información Documentos que conforman el expediente contractual (Formatos, minutas, actas, comunicaciones y demás que se expidan con ocasión a la ejecución del contrato/convenio)
Riesgo	Posibilidad de Perdida de Integridad por fallas humanas o destrucción de la información o error en el uso o abuso de derechos y privilegios o falsificación de derechos de acceso de documentos que conforman el expediente contractual (formatos, minutas, actas, comunicaciones y demás que se expidan con ocasión a la ejecución del contrato/convenio),
Causa	Debido al manejo manual de la información o ausencia de copias de respaldo de la información o ausencia de validación de autenticación de la información o retraso en la entrega de información por parte del personal o insuficiente entrenamiento y capacitación sobre políticas de seguridad y privacidad de la información o ausencia o deficiencia en los sistemas de autenticación de los aplicativos.
Objetivo de Control 1	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Control	El líder del proceso de "Administración del Talento Humano", realiza anualmente sesiones de inducción y reinducción a los colaboradores de la SDP, para socializar los lineamientos de la entidad a nivel de Sistema de Gestión.
Objetivo de Control 2.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control	El líder del proceso de "Soporte Tecnológico", realiza periódicamente durante la vigencia las copias de respaldo de la información de las carpetas o sitios compartidos, así como de los equipos de cómputo de la SDP (según solicitud)
Objetivo de Control 3.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
Control	El responsable de la contratación (dependencia solicitante), debe propender por que la información a tramitar corresponda con los documentos o lineamientos internos dados por el proceso de "Contratación de Bienes y Servicios".
Objetivo de Control 4.	La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
Control	El responsable de la contratación (dependencia solicitante), debe dar cumplimiento a los plazos pactados para el inicio del proceso contractual, así como de la atención de los requerimientos que realice el equipo de la Dirección de Contratación - líder del proceso de "Contratación de Bienes y Servicios".
Objetivo de Control 5.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo
Control	El líder del proceso de "Administración del Talento Humano", realiza anualmente sesiones de inducción y reinducción a los colaboradores de la SDP, para socializar los lineamientos de la entidad a nivel de Sistema de Gestión.
Objetivo de Control 6.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	El líder del proceso de "Soporte Tecnológico", ejecuta durante la vigencia el plan de sensibilización de Seguridad de la Información al interior de toda la entidad.

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presenta niveles de criticidad medio, Se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo se debe gestionar dichos riesgos. Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, no se detalla que pasa si el control falla. En la descripción del control se evidencian frecuencias anuales, periódicas y en otras no determina la periodicidad sin embargo en la matriz de riesgos, hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Finalmente, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación.

4.3.4 PROCESO CONTROL INTERNO DISCIPLINARIO S-CA-003

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Oficina de Control Interno Disciplinario
Nuevo Proceso	S-CA-003 CONTROL INTERNO DISCIPLINARIO
Objetivo del Proceso	Ejercer la acción disciplinaria e implementar estrategias que fortalezcan la conducta de los servidores de la SDP, mediante la aplicación de la Constitución Política, las leyes vigentes, la autorregulación y el Código de Integridad de la Entidad, así como la determinación, diseño y ejecución de actividades preventivas que mitiguen la comisión de faltas disciplinarias y promuevan el cabal cumplimiento de los fines institucionales.

Tipo de Riesgo	**Gestión**
Riesgos	Posibilidad de afectación reputacional por ejercer inadecuadamente la potestad disciplinaria.
Causas	Interpretación equívoca de la ley, insuficiente capacitación y actualización a los funcionarios de la Oficina de Control Disciplinario Interno y Subsecretaría Jurídica en los temas propios del proceso disciplinario, así como la prescripción y caducidad del mismo.

Conclusiones: Se suguiere verificar tanto la redacción de los riesgos como la identificación de nuevos riesgos y causas, así como de controles que mitiguen dichos riesgos, contemplando actividades o estrategias para fortalecer la conducta de los servidores de la SDP, Posibilidad de prescripción y/o caducidad de la acción disciplinaria, obstrucción al curso de las investigaciones, de violación de los términos legales y toma de decisiones no adecuadas entre otras.

Tipo de Riesgo	**Corrupción**
Riesgos	Posibilidad de trámite indebido de quejas, informes, denuncias y procesos disciplinarios en beneficio de un tercero
Causas	1. Amiguismo para influenciar los trámites y resultados de los procesos disciplinarios. 2. Interés propio o de un tercero en direccionar el resultado de los procesos disciplinarios

Conclusiones: El control hace referencia a la asignación de confidencialidad de los documentos generados al interior de la oficina en el aplicativo SIPA y no está mitigando las causas del riesgo como lo puede ser el amiguismo interés propio o de un tercero para influenciar en los tramites y el resultado de los procesos disciplinarios. Por otra parte, se sugiere fortalecer el plan de acción de la vigencia 2024, para el tratamiento del riesgo que realmente mitigue dicho riesgo y no solo se contemple realizar de una capacitación dirigida al personal de la Oficina de Control Disciplinario Interno a fin de verificar la apropiación en los temas referentes a los actos de corrupción.

Tipo de Riesgo	**Seguridad de la Información**
Tipo de Activo	Datos Información Procesos Disciplinarios
Riesgo	Posibilidad de Pérdida de Confidencialidad por fallas humanas y hurto de información de los procesos disciplinarios,
Causa	Debido al desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, manejo manual de la información, ausencia de copias de respaldo o Backus de la información, copias no controladas e información sensible sin cifrado
Objetivo de Control 1.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo
Control	Los funcionarios y contratistas son responsables de participar activamente en los procesos de sensibilización, liderados por el equipo de seguridad de la información de la entidad, por lo menos una vez en el semestre.
Objetivo de Control 2.	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
Control	El jefe de la Oficina de Control Disciplinario Interno periódicamente revisa que los funcionarios y contratistas cumplan con las disposiciones legales dentro del proceso disciplinario
Objetivo de Control 3.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control	El proceso Soporte Tecnológico realiza la actividad de respaldo de la información de acuerdo a la política A-LE-297 y al procedimiento A-PD-092, definido por el sistema de seguridad de la información
Objetivo de Control 4:	Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
Control	Los funcionarios y contratistas son responsables de aplicar la política de medio a removibles A-LE-320 definida por el sistema de seguridad de la información

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presenta niveles de criticidad medio, Se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo se debe gestionar dichos riesgos. Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, delimitar el responsable del control para el caso del *proceso*

Soporte Tecnológico es importante establecer el cargo (profesional, técnico, coordinador o jefe) que realiza no se puede generalizar y detallar qué pasa si el control falla.

Por otra parte, en la descripción del control se evidencian frecuencias semestrales, periódicas y en otras no determina la periodicidad, sin embargo, en la matriz hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Adicionalmente, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación. En cuanto al segundo control identificado y teniendo en cuenta que su zona de riesgo residual es ALTO no se registra plan de acción para el tratamiento del riesgo indicando la actividad, responsable, fecha de implementación y de seguimiento.

Finalmente, atender lo indicado en el *Informe de Auditoría de Sistemas de Gestión* de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

4.3.5 PROCESO COORDINACIÓN DE POLÍTICAS PÚBLICAS Y DE INSTRUMENTOS DE PLANEACIÓN – M-CA-002

Objetivo Estratégico	1. Fortalecer la formulación, seguimiento y evaluación de planes, programas, políticas y proyectos en la ciudad en materia económica, social y ambiental de forma coordinada y articulada con los actores de Bogotá Región. 3. Liderar la formulación, seguimiento y evaluación de la inversión pública, generando insumos para la toma de decisiones, que permitan maximizar el impacto de las inversiones en el territorio.
Líder Proceso	Subsecretaría de Políticas Públicas y Planeación Social y Económica
Procesos Nuevo	M-CA-006 POLÍTICAS PÚBLICAS (PP)
Objetivo del Proceso	Direccionar la formulación, ejecución, seguimiento y actualización de la planeación institucional a nivel estratégico, táctico y operativo mediante la definición e implementación de lineamientos e instrumentos de planeación, que permitan lograr el cumplimiento de la misión, visión y compromisos del plan distrital de desarrollo, facilitando la toma de decisiones, contribuyendo a la mejora continua y generando valor público.
Líder Proceso	Oficina de Integración Regional
Procesos Nuevo	E-CA-010 ARTICULACIÓN DEL DIÁLOGO SUPRADISTRITAL
Objetivo del Proceso	Apoyar al Despacho en la coordinación de las acciones del Distrito Capital con las figuras de gobernanza supradistrital y las entidades territoriales que permita la construcción de un desarrollo sostenible, equilibrado y descentralizado.
Objetivo Estratégico	3. Liderar la formulación, seguimiento y evaluación de la inversión pública, generando insumos para la toma de decisiones, que permitan maximizar el impacto de las inversiones en el territorio.
Líder Proceso	Subsecretaría de Planeación de la Inversión
Proceso Nuevo	M-CA-004 PLAN DE DESARROLLO DISTRITAL (PDD)
Objetivo del Proceso	Coordinar y dar los lineamientos para la formulación, ejecución y seguimiento de los planes de desarrollo distrital y locales y los proyectos de inversión.

El proceso M-CA-006 *Políticas Públicas (PP)* con el rediseño institucional se dividió en 3 procesos. Sin embargo, dentro de los mapas de riesgos que se han actualizado, no se observan riesgos directamente asociados al proceso E-CA-010 *Articulación del Diálogo Supradistrital* a cargo de la Oficina de Integración Regional, el cual actualmente se está ejecutando sin que se evidencie la gestión de riesgos desarrollada.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación reputacional por desacierto en el seguimiento de política pública, debido a:
Causas	1. Inexistencia y/o desactualización de los sistemas de información y/o de los instrumentos de seguimiento de políticas públicas 2. Ausencia de oportunidad y calidad en la presentación de los informes de seguimiento a los planes de acción de las políticas pública por parte de algunos sectores rectores de política.
Controles	1. El profesional de la Dirección de Formulación y Seguimiento de Políticas Públicas cada vez que se requiera verifica que la política pública se formule de acuerdo con los elementos de la Guía para la formulación e implementación de políticas públicas del Distrito, su caja de herramientas y los lineamientos para la Participación Ciudadana, a través del formado A-FO-184 de seguimiento de reuniones. En caso de encontrar información faltante, requiere al sector a través de correo para ajuste de los documentos y poder continuar con el proceso. 2. El profesional de la Dirección de Formulación y Seguimiento de Políticas Públicas trimestralmente valida los criterios definidos para el reporte cualitativo y cuantitativo, de acuerdo a la cadena de valor del producto y resultado y con la información que se debe asociar a los enfoques definidos, valor de meta programado, línea base y tipo de anualización a través del Sistema de Seguimiento y Evaluación de Política Pública. Para las inconsistencias en la información presentadas, requiere al sector a través de correo electrónico para ajuste de la información. Como evidencia se encuentra el correo de solicitud de información y el informe respectivo.

Conclusiones: Se recomienda la revisión del segundo control de este riesgo, ya que fue catalogado como correctivo, sin que se relacionara con la gestión en el evento de una materialización de riesgos.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación reputacional por debilidad en el proceso de formulación e implementación de políticas públicas e instrumentos de planeación, debido a
Causas	1. Modificación de lineamientos técnicos de acuerdo con los cambios en la administración de grupos de valor 2. Invisibilización de los grupos poblacionales en algunos espacios de la agenda pública e incumplimiento por parte de las entidades distritales de los lineamientos y/o circulares establecidas por la SDP
Controles	1. El profesional de la Dirección de Formulación y Seguimiento de Políticas Públicas cada vez que se requiera verifica que la política pública se formule de acuerdo con los elementos de la Guía para la formulación e implementación de políticas públicas del Distrito, su caja de herramientas y los lineamientos para la Participación Ciudadana, a través del formado A-FO-184 de seguimiento de reuniones. En caso de encontrar información faltante, requiere al sector a través de correo para ajuste de los documentos y poder continuar con el proceso. Como evidencia se encuentra el correo de solicitud de información o el A-FO-184.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación reputacional por debilidad en el proceso de formulación e implementación de políticas públicas e instrumentos de planeación, debido a
	2. El Director(a) de la Dirección de Formulación y Seguimiento de Políticas Públicas cada vez que se requiera valida la revisión de la política pública que realizó el profesional de la dirección, con el fin de analizar las causas de las desviaciones en la formulación y comunica al responsable para adelantar las acciones correspondientes según sea el caso. Como evidencia se encuentran los comunicados realizados y las respuestas emitidas y el diligenciamiento del E-FO-062 Control de la Salida, Producto y/o Servicio no Conforme. 3. El profesional de la Dirección de Formulación y Seguimiento de Políticas Públicas cada vez que se requiera revisa si la política pública se adoptó mediante acto administrativo (Decreto o Acuerdo Distrital) anterior a reglamentación del CONPES, si cuenta con concepto de viabilidad en fase preparatoria, con documento de diagnóstico e Identificación de factores estratégicos o documento CONPES y formulación del plan de acción aprobado, a través de la matriz de inventario de políticas públicas. La verificación permitirá establecer con precisión la ubicación de la política en el ciclo y las actividades de asistencia técnica que puede requerir. Como evidencia se encuentra la matriz de inventario de políticas públicas, el A-FO-184 de registro de reuniones y el concepto técnico.

Conclusiones: Se recomienda la revisión del segundo control de este riesgo, ya que fue catalogado como correctivo, sin que se relacionara con la gestión en el evento de una materialización de riesgos.

Durante la vigencia 2023 se identificaron 4 hallazgos resultado de 2 informes de la Contraloría de Bogotá, relacionados con los riesgos de gestión, atendiendo a que se refieren a formulación y seguimiento a las políticas públicas, como se muestra a continuación:

Tabla N. 1. Hallazgos generados por la Contraloría de Bogotá relacionados con el riesgo

Informe	Hallazgo
Informe de auditoría de desempeño Contraloría de Bogotá, Coordinada por la Auditoría General de la Nación Argentina Políticas implementadas para el logro de las metas del ODS 1 y mitigación de impacto COVID-19, con énfasis en la disminución de brechas de género en Bogotá. Vigencias 2020 y 2021(2023)	2158. 3.1.2 Hallazgo administrativo por vacíos en la metodología del CONPES D.C., respecto a la definición de líderes de política pública en procesos de reformulación y la finalización del trámite de una iniciativa de política pública que no culmina en Documento CONPES D.C.
	2159. 3.1.3 Hallazgo administrativo por fallas en las políticas públicas para grupos étnicos y en la coherencia horizontal de los instrumentos de planeación, lo que dificulta la identificación de su aporte al cumplimiento de la Agenda 2030.
	2160 3.2.2 Hallazgo administrativo por debilidades en el seguimiento de las políticas públicas, grupos étnicos y derechos humanos, así como la falta de información sobre el avance alcanzado en el enfoque de género
Informe de Auditoría de Regularidad de la Contraloría de Bogotá Secretaría Distrital de Planeación, Código de Auditoría No. 46 PAD 2023.	2148 3.2.3.1 Hallazgo administrativo con presunta incidencia disciplinaria por deficiencias en la adopción y seguimiento del plan de acción de la Política Pública Distrital de Espacio Público

Fuente: SIPA- Módulo Planes de Mejoramiento. Reporte Matriz Todo

Se realizó la evaluación de la aplicación de los controles con corte a abril de 2024. Para el primer riesgo, con relación al primer control definido en el mapa de riesgos con frecuencia continuo, sin embargo, la evidencia sólo reporta a este corte un acta de reunión "*Revisión de reportes y alcances de la política de Actividades Sexuales Pagadas con corte a diciembre 2023"* realizada el 24 de abril de 2024. Tal como lo indicó la segunda línea defensa en su informe, no es posible establecer la aplicación continua del control, adicionalmente se presume que la actividad debe

hacerse para las políticas vigentes, sin embargo, en esta acta sólo se trató una política. Para el segundo control, se recomienda que dado que en la evidencia SDP-2024-4276 se adjuntan 44 planes de acción con el seguimiento realizado, no se observa la forma en que se da a conocer y se hacen seguimiento a los diferentes sectores encargados de las políticas evaluadas.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación reputacional por emisión de conceptos de traslado presupuestal a los fondos de desarrollo local sin cumplimiento de requisitos de los conceptos de gasto, debido a:
Causas	La carencia de un repositorio que concentre el conocimiento funcional del equipo ejecutor del proceso y de buenas prácticas y lecciones aprendidas pese a la consolidación de procesos, procedimientos, guías metodológicas, formatos a nivel institucional como herramientas reconocidas.
Controles	1. El profesional de la Dirección de Programación, Seguimiento a la Inversión y Planes Desarrollo Locales valida que la solicitud de concepto de traslado y sus soportes adjuntos, sustenten el cumplimiento de lineamientos del CONFIS Distrital, el manual de presupuesto (de Hacienda) y los Criterios de Elegibilidad y Viabilidad Técnica y de incorporación de enfoques poblacionales (de los sectores lideres de los conceptos del gasto afectados), caso contrario, gestiona con el Fondo de Desarrollo Local solicitante del concepto (vía correo electrónico) la actualización de la información que sustenta la solicitud. 2. El profesional de la Dirección realiza la revisión con base en el procedimiento M-PD-206 "Concepto sobre modificaciones al presupuesto de inversión local", específicamente, el insumo descrito como "Documentos y anexos específicos que debe contener la solicitud" y el numeral 4 de las observaciones generales. 3. El Director de Programación, Seguimiento a la Inversión y Planes Desarrollo Locales revisa que el concepto se encuentre debidamente sustentado, analizado y conforme a los lineamientos vigentes, caso contrario, revisa y brinda instrucciones al profesional designado en la dirección (vía SIPA) de los ajustes a aplicarse al contenido del concepto. 4. Esta revisión incluirá la verificación en el marco del procedimiento M-PD-206 "Concepto sobre modificaciones al presupuesto de inversión local", específicamente, el insumo descrito como "Documentos y anexos específicos que debe contener la solicitud" y el numeral 4 de las observaciones generales" 5. El profesional de la Dirección de Programación, Seguimiento a la Inversión y Planes Desarrollo Locales analiza el concepto y el dato aparentemente errados, si es necesario contacta al Fondo de Desarrollo Local para analizar su incidencia (vía correo electrónico), le solicita los ajustes a que haya lugar en la solicitud y procede a emitir nuevo concepto como alcance al concepto inicial, caso contrario, proyecta comunicación (vía SIPA) absteniéndose de emitir concepto favorable. 6. Esta revisión incluirá la verificación en el marco del procedimiento M-PD-206 "Concepto sobre modificaciones al presupuesto de inversión local", específicamente, el insumo descrito como "Documentos y anexos específicos que debe contener la solicitud" y el numeral 4 de las observaciones generales"

Conclusiones: Se recomienda la revisión del primer control de este riesgo, ya que fue catalogado como correctivo, sin que se relacionara con la gestión en el evento de una materialización de riesgos. Igualmente, se sugiere el análisis de controles encaminados a subsanar la causa raíz referida a la carencia de un repositorio que concentre el conocimiento funcional del equipo.

Tipo de Riesgo	Corrupción
Riesgo	Posibilidad de uso del poder en el proceso de política pública por el rol de la SDP en el liderazgo y coordinación del ciclo de políticas públicas, por el creciente interés de diferentes actores en los temas de planificación, ordenamiento y renovación urbana.
Causas	1. Influencia de un tercero por intereses de actores que presionen la toma de decisiones a favor de una actuación o procedimiento. 2. Vacíos en la interpretación de la norma. 3. Dificultad en la aplicación de la norma. 4. Motivación u orientación personal de un servidor de la SDP
Controles	1. Los profesionales del proceso verifican cada vez que se requiera durante el ciclo de formulación y seguimiento de políticas públicas, el cumplimiento de la guía de formulación e implementación de política pública y la caja de herramientas, a través de la realización de mesas o talleres de trabajo. En caso de no cumplir con los lineamientos establecidos en la guía, hacen la observación correspondiente. Como evidencia se encuentra el A-FO-184 de seguimiento de reuniones y correos electrónicos. 2. El Director de Formulación y Seguimiento de Políticas Públicas revisa cada vez que se requiera durante el ciclo de formulación políticas públicas, el concepto técnico unificado de la SDP sobre la propuesta de estructuración de la política pública. En caso de no cumplir con los parámetros solicitados, hace la observación correspondiente. Como evidencia se encuentran los correos electrónicos.

Conclusiones: La Oficina de Control Interno considera importante incluir dentro de los controles el análisis de la declaración de conflictos de intereses que se puedan generar tanto por parte de los profesionales que realizan labores de seguimiento y monitoreo y extensiva a las entidades líderes de las políticas públicas. La aplicación de los 2 controles establecidos se limita a la expresión *"cada vez que se requiera"* de lo cual se sugiere la revisión, a fin de que se establezca una periodicidad acorde al desarrollo del ciclo de las políticas públicas.

Tipo de Riesgo	Información
Activo de Información	Datos Información: Conceptos técnicos
Riesgo	Posibilidad de Perdida de Integridad por fallas humanas; de conceptos técnicos, debido a
Causas	Insuficiente entrenamiento y capacitación sobre políticas las de seguridad y privacidad de la información
Objetivo de Control 1	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización
Control 1	Los directivos del proceso revisan y validan los contenidos de los conceptos antes de su emisión final.
Objetivo de Control 2	La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
Control 2	El Líder del proceso vela porque todos sus procedimientos se conozcan y se cumplan aplicando los lineamientos establecidos en la política A-LE 429 Políticas de seguridad y privacidad de la información.

Tipo de Riesgo	Información
Activo de Información	Datos Información: No se define
Riesgo	Posibilidad de pérdida de disponibilidad por:
Causas	1. Fallas Humanas; de activos de información, 2. Manejo manual de la información, 3. Ausencia de copias de respaldo o backup de la información
Objetivo de Control 1	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control 1	Los colaboradores del proceso conocen y aplican los lineamientos establecidos en la política A LE 429 Políticas de seguridad y privacidad de la información.
Objetivo de Control 2	La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
Control 2	Los colaboradores del proceso conocen y aplican los procedimientos documentados, así como las directrices de conservación de los registros productos de los mismos.

Conclusiones: Se sugiere el fortalecimiento de los controles atendiendo las características de un control (responsable, periodicidad, propósito, evidencia) definidas en la *E-LE-030 Política de administración del riesgo* y la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* en su versión 4, a fin de salvaguardar la integridad y disponibilidad de los activos, atendiendo tanto el activo en su forma digital como física.

Por otra parte, para el riesgo *Posibilidad de Perdida de Integridad por fallas humanas; de conceptos técnicos*, no se identificó el activo de información dentro del A-LE-283 *Registro de activos de información (RAI),* y para el riesgo *Posibilidad de pérdida de disponibilidad* no se incluye el activo al que se refiere el riesgo. Así mismo, en el A-LE-283 no se identificó ningún activo con nivel de criticidad Alta. Adicionalmente, se recomienda la revisión del *M-LE-223 Mapa de Riesgos de Seguridad de la Información del Proceso Coordinación de las Políticas Públicas y de los Instrumentos de Planeación*, a fin de que muestre la *Evaluación del Riesgo - Nivel del Riesgo Residual* por riesgo y no por cada control como está apareciendo actualmente.

4.3.6 PROCESO DIRECCIONAMIENTO ESTRATÉGICO - E-CA-001

Objetivo Estratégico	4. Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Área Responsable	Dirección de Planeación Institucional
Proceso Nuevo	E-CA-004 DIRECCIÓN ESTRATÉGICA INSTITUCIONAL
Objetivo del Proceso	Direccionar la formulación, ejecución, seguimiento y actualización de la planeación institucional a nivel estratégico, táctico y operativo mediante la definición e implementación de lineamientos e instrumentos de planeación, que permitan lograr el cumplimiento de la misión, visión y compromisos del plan distrital de desarrollo, facilitando la toma de decisiones, contribuyendo a la mejora continua y generando valor público.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por la definición, orientación y coordinación de la planeación institucional desarticulada de los lineamientos distritales y nacionales, debido a:
Causas	1. Bajo nivel de apropiación de las metodologías e instrumentos para la planeación estratégica, operativa y del Sistema de Gestión de la entidad 2. Dificultad en la interacción de los procesos 3. Debilidad en la cultura de planeación.
Controles	1. Los profesionales de la Dirección de Planeación Institucional verifican cada vez que se requiera en los aplicativos de la entidad, el cumplimiento de los lineamientos para la planeación institucional de la Secretaría Distrital de Planeación (E-IN-011) y demás documentos del proceso, con el fin de articular y alinear las acciones para apoyar la toma de decisiones en el corto, mediano y largo plazo. Si se evidencia alguna inconsistencia, se informa a la dependencia correspondiente, a través de un medio oficial de comunicación, con el fin de tomar las acciones correctivas. 2. El(la) Director(a) de Planeación Institucional valida cada vez que se requiera en los reportes que se generan de los aplicativos de la entidad, la información de la planeación institucional con el fin de monitorear el estado de avance de dicha planeación. Las situaciones de alerta, las informa al profesional de la dirección que asesora el respectivo proceso, para que gestione lo pertinente frente a la situación encontrada. 3. El Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Planeación revisa y analiza cada vez que se requiera, la información correspondiente a la planeación institucional con el fin de realizar las recomendaciones y tomar las decisiones que se requieran, en aras de propender por el cumplimiento de las metas e indicadores planeados, dichas decisiones quedan consignadas en las actas de cada reunión.

Conclusiones: Los controles establecidos para este riesgo se enfocan principalmente al análisis de la información cargada en los aplicativos. Sin embargo, la Oficina de Control Interno considera relevante, atacar también las causas referentes a *Dificultad en la interacción de los procesos* y *Debilidad en la cultura de planeación*, dado que aunque no se han establecido hallazgos, sí se han registrado recomendaciones y situaciones susceptibles de mejora en los informes de esta Oficina, que han evidenciado falta de articulación entre los procesos, como es el caso del manejo de PQRS y los planes de mejoramiento estructurados para su tratamiento. Por otra parte, en cuanto a debilidades en la cultura de planeación, esta Oficina también ha detectado falencias en cuanto a la planeación de los procesos contractuales y de algunas acciones de planes de mejoramiento que han requerido solicitud de prórroga. En este punto es importante hacer mención del rediseño institucional, dado que, en octubre de 2022 se modificó la estructura organizacional y consecuente generación de nuevo mapa de procesos, sin que a la fecha se cuente con el sistema de gestión actualizado. Por lo anterior, se recomienda tener en cuenta estas situaciones en la estructuración de los riesgos.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por desempeño de los procesos y resultados de los proyectos en un nivel inferior al esperado, debido a:
Causas	1. Incumplimiento de la Planeación Estratégica y Plan de Desarrollo, 2. Debilidad en la articulación de los instrumentos de planeación interna (Plan de Contratación, Plan de Acción, POA, Plan Estratégico, Planes de Mejoramiento, Mapa de Riesgos), 3. Deficiencias en la calidad y oportunidad de la información reportada por los procesos

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por desempeño de los procesos y resultados de los proyectos en un nivel inferior al esperado, debido a:
	4. Dificultad en la interacción de los mismos.

Conclusiones: Se sugiere mejorar la redacción del riesgo dado que la inclusión de las 4 causas dentro de su texto hace más compleja su comprensión. Adicionalmente, no se observa con claridad que los controles establecidos ataquen todas las causas definidas, vale decir para el caso de *Debilidad en la articulación de los instrumentos de planeación interna (Plan de Contratación, Plan de Acción, POA, Plan Estratégico, Planes de Mejoramiento, Mapa de Riesgos)* y *Dificultad en la interacción de los procesos.*

Por otra parte, la Contraloría de Bogotá en su *Informe de Auditoría de Regularidad de la Contraloría de Bogotá Secretaría Distrital de Planeación, Código de Auditoría No. 46 PAD 2023,* estableció el hallazgo *"3.2.1.1 Hallazgo administrativo por el incumplimiento del principio de planeación para la ejecución de la meta 10 del proyecto 7631, en la vigencia 2022.",* para el cual se establecieron 2 acciones, una de ellas a cargo de la Dirección de Planeación Institucional. Sin embargo, en el *"Informe monitoreo de segunda línea de defensa a los mapas de riesgos de gestión, corrupción y de seguridad de la información de la secretaría distrital de planeación corte a 31 de agosto de 2023",* indica que para el caso de este mapa de riesgos *"con corte al 31 de agosto no se cuenta con hallazgos de auditoría asociados a los controles identificados en el mapa de riesgos del proceso.".* Dado lo anterior, la Oficina de Control Interno invita a tener en cuenta los hallazgos que se han generado en la entidad como fuente esencial de insumo, a fin de fortalecer la estructuración de los riesgos y consecuentemente los controles para su tratamiento.

Tipo de Riesgo	Información
Activo de Información	Datos Información. Resoluciones y/o Actas de Mejoramiento anteriores al año 2012
Riesgo	Posibilidad de Pérdida de Disponibilidad por:
Causas	1. Fallas humanas relacionadas a las resoluciones y/o Actas de Mejoramiento anteriores al año 2012 debido a 2. Manejo manual de la información
Objetivo de Control 1	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
Control 1	El enlace SG-MIPG de la Dirección de Planeación verifica anualmente en el A-FO-209 Formato Registro de Activos de Información que se encuentren relacionados y clasificados los activos de información de la dependencia, con el fin de actualizarla y remitirla a la Dirección de Sistemas para su consolidación.
Objetivo de Control 2	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
Control 2	El auxiliar administrativo de la Dirección de Planeación Institucional revisa cada vez que se requiera, que el lugar de almacenamiento de los documentos permanezca cerrado con el fin de controlar el acceso a la información física de la dependencia. Las novedades se informan al Director (a) de Planeación.

Conclusiones: No se observa la relación directa del primer control con las causas y el riesgo. Adicionalmente, se observa que el control no se está cumpliendo, dado los activos de información no se han actualizado. Se sugiere orientar la redacción del riesgo a la pérdida de disponibilidad y

de integridad del activo o su deterioro, así como los controles. Por otra parte, se recomienda la revisión del A-LE-518 *Mapa de Riesgos de Seguridad de la Información del Proceso Administración del Talento Humano,* a fin de que muestre la *Evaluación del Riesgo - Nivel del Riesgo Residual* por riesgo y no por cada control como está apareciendo actualmente.

Tipo de Riesgo	Información
Activo de Información	Información reportada de los resultados de la gestión institucional
Riesgo	Posibilidad de Pérdida de integridad por:
Causas	1. Fallas humanas 2. Falsificación de derechos de acceso relacionadas con la información reportada de los resultados de la gestión institucional 3. Ausencia de validación de autenticación y deficiencia en la autorización de permisos de la información

Conclusiones: No fue posible identificar el activo aquí definido en el A-LE-283 *Registro de activos de información* (RAI), además que para el caso de la Dirección de Planeación Institucional solo se relaciona un activo con nivel de criticidad ALTO y corresponde a *"Resoluciones anteriores al 30 de noviembre de 2010 y Actas de mejoramiento y control de documentos del Sistema de gestión de la SDP anteriores al año 2012 y sus anexos (caracterizaciones de procesos, procedimientos, formatos, instructivos, documentos línea estratégica, fichas técnicas de comités y hojas de vida de Gobierno en Línea e indicadores y caracterizaciones de producto)"*.

Por otra parte, se recomienda la revisión del A-LE-518 *Mapa de Riesgos de Seguridad de la Información del Proceso Administración del Talento Humano,* a fin de que muestre la *Evaluación del Riesgo - Nivel del Riesgo Residual* por riesgo y no por cada control como está apareciendo actualmente. Adicionalmente, se observan casillas en EVALUACIÓN DEL RIESGO - NIVEL DEL RIESGO RESIDUAL cuyo tratamiento es *Reducir* sin que se establezca el plan de acción respectivo.

Tipo de Riesgo	Corrupción
Riesgo	Posibilidad de manipulación de la información relacionada con la planeación, inversión, resultados y metas para favorecer a terceros
Causas	1. Presiones de funcionarios con poder de decisión para ajustar resultados de la gestión. 2. Desarticulación de la planeación contractual con la formulación de proyectos. 3. Información generada y /o enviada por las dependencias que no se ajuste a la realidad de la gestión institucional.
Controles	1. El equipo de profesionales de la Dirección de Planeación Institucional verifica trimestralmente en el reporte del aplicativo SIPG, que el avance sea coherente con lo programado frente a las metas, indicadores y productos, con el fin de medir el grado de ejecución de lo planificado. Si existe alguna inconsistencia, se informa a la dependencia correspondiente, a través de un medio oficial de comunicación en la entidad, para gestionar las acciones correctivas correspondientes. 2. El Profesional de la Dirección de Planeación Institucional revisa cada vez que se requiera, la información publicada en la página web de la SDP, con el fin de verificar el cumplimiento de la Ley de Transparencia. Si hay alguna inconsistencia u observación, se informa al profesional y/o al Director(a) de Planeación Institucional por cualquier medio de comunicación establecido con el fin de gestionar los ajustes correspondientes. 3. El Director(a) de Planeación Institucional verifica cada vez que se requiera, los reportes correspondientes, los lineamientos de la planeación y el seguimiento a los Planes

Tipo de Riesgo	Corrupción
Riesgo	Posibilidad de manipulación de la información relacionada con la planeación, inversión, resultados y metas para favorecer a terceros
	Operativos, con el fin de validar que los mismos se articulen con el Plan Estratégico de la entidad. Si se evidencia alguna inconsistencia se informa al profesional de su dirección para gestionar los ajustes correspondientes.

Conclusiones: Dada la transversalidad del riesgo, se sugiere que los controles incluyan también a la primera línea de defensa quien en la mayoría de los casos es el responsable de la información. Por otra parte, se considera importante incluir controles que ataquen la segunda causa raíz definida, referente a desarticulación de la planeación contractual con la formulación de proyectos, dado que la Oficina de Control Interno en los Seguimientos a la Ejecución de los Compromisos de la SDP en el PDD 2020 – 2024, ha identificado situaciones susceptibles de mejora relacionados con esta situación.

Tipo de Riesgo	Corrupción
Riesgo	Posibilidad de desviación de la gestión en la asignación, programación y ejecución presupuestal con destinación diferente al cumplimiento de las metas y programas institucionales para favorecimiento de terceros.
Causas	1. Manipulación de la información para la formulación de estrategias, planes, programas y proyectos. 2. Presiones de funcionarios con poder de decisión para ajustar resultados de la gestión. 3. Debilidad en la aplicación de los instrumentos que permitan verificar la coherencia entre la contratación y el cumplimiento de las metas 4. Presiones de las partes interesadas con poder de decisión para contratar bienes y servicios.
Controles	1. El profesional de la Dirección de Planeación Institucional verifica cada vez que se requiera en el Certificado de Registro Presupuestal y en el Plan Anual de Adquisiciones, que el objeto contractual esté articulado con las metas de inversión, con el fin de determinar la viabilidad técnica de los proyectos de inversión y su adecuada formulación técnica. Si hay inconsistencias, informa al Director(a) de Planeación Institucional, para que este comunique al área correspondiente a través de un medio oficial de comunicación en la entidad. 2. El Profesional de la Dirección de Planeación Institucional verifica cada vez que se requiera, a cuáles metas del Plan de Desarrollo Distrital contribuye la SDP en el marco de sus competencias, para determinar que el proyecto de inversión, la ficha EBI y el plan de acción cumplan con la metodología vigente de conformidad con el procedimiento E-PD-029 Gestión de Proyectos de Inversión de la SDP. Todas las observaciones encontradas son informadas al Director(a) de Planeación Institucional través de un medio oficial de comunicación en la entidad, con el fin de tomar acciones en caso al que haya lugar. 3. El Director(a) de Planeación Institucional valida anualmente en los soportes internos, el cumplimiento de las directrices para la programación presupuestal de la siguiente vigencia emitidas en Circular conjunta por la Secretaría Distrital de Hacienda y la Secretaría Distrital de Planeación para la construcción del Anteproyecto de Presupuesto. Si se evidencia alguna inconsistencia, se informa al área correspondiente a través de un medio oficial de comunicación en la entidad, para que realice los respectivos ajustes. 4. El Director(a) de Planeación Institucional valida cada vez que se requiera, el estado y ejecución de los proyectos de inversión en los reportes que genera el aplicativo distrital

Tipo de Riesgo	**Corrupción**
Riesgo	Posibilidad de desviación de la gestión en la asignación, programación y ejecución presupuestal con destinación diferente al cumplimiento de las metas y programas institucionales para favorecimiento de terceros.
	de Seguimiento al Plan de Desarrollo - SEGPLAN, con el fin de asegurar la confiabilidad de la información en el avance de los proyectos y metas del Plan de Desarrollo. Si detecta una situación de alerta, informa al área correspondiente a través de un medio oficial de comunicación en la entidad.

Conclusiones: Dada la transversalidad del riesgo, se sugiere que los controles incluyan también a la primera línea de defensa quien en la mayoría de los casos es el responsable de la información. Se sugiere cambiar la redacción del control para que no se aplique cada vez que se requiera sino de forma permanente a todos los procesos contractuales referentes a recursos de inversión. Por otra parte, se considera importante incluir controles que ataquen la tercera causa raíz definida, referente a debilidad en la aplicación de los instrumentos que permitan verificar la coherencia entre la contratación y el cumplimiento de las metas, dado que la Oficina de Control Interno en los Seguimientos a la Ejecución de los Compromisos de la SDP en el PDD 2020 – 2024, ha identificado situaciones susceptibles de mejora relacionados con esta situación. Por otra parte, se sugiere fortalecer el plan de acción establecido, dado que se orienta únicamente a realizar sensibilizaciones.

4.3.7 PROCESO DE EVALUACIÓN Y CONTROL S-CA-001

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Oficina de Control Interno
Proceso	Nuevo: S-CA-004 EVALUACIÓN Y CONTROL
Objetivo del Proceso	Proveer aseguramiento, asesoría y análisis basados en riesgos, de forma independiente y objetiva, a través del liderazgo estratégico, evaluación y seguimiento, enfoque hacia la prevención, evaluación a la gestión del riesgo y relación con entes externos de control y vigilancia, con el fin de proteger el valor de la entidad y mejorar la eficacia de las actividades de gestión de riesgos, control y gobierno

Tipo de Riesgo	**Gestión**
Riesgos	Posibilidad de afectación reputacional por informes emitidos por la oficina de control interno que contengan información de fuentes que no se ajustan a la realidad de la entidad.
Causas	información errónea o incompleta suministrada por los auditados para la evaluación del sistema de control interno

Conclusiones: Se sugiere revisar la identificación de nuevos riesgos, causas y controles o fortalecer los ya existentes, contemplando la posibilidad de incumplir el Plan Anual de Auditoría , por la no ejecución de actividades programadas, debido a la no disponibilidad de recursos, también por la Posibilidad de inconsistencias en la ejecución de la auditoria por falta de equipo auditor con el perfil requerido para atender la auditoría, disponibilidad de tiempo de los auditados para la atención de la auditoría con calidad y oportunidad.

Tipo de Riesgo	**Corrupción**
Riesgos 1.	Posibilidad de omitir o incluir información en beneficio propio o de un tercero que afecte intencionalmente la evaluación independiente al Sistema de Control Interno, al omitir o encubrir hechos irregulares detectados.
Causas	1. Conflicto de intereses no manifestados. 2. Ceder ante las presiones. 3. Incumplimiento del código de ética.

Conclusiones: se sugiere revisar los controles identificados conforme a las causas Conflicto de intereses no manifestados, Ceder ante las presiones e Incumplimiento del código de ética (en temas de integridad, independencia y objetividad, confidencialidad y reserva, competencia y respecto entre colegas) que efectivamente mitigue dicho riesgo y que ataque estas causas originadoras del riesgo, a su vez contemplar riesgos por solicitar o aceptar comisión, extorsión o recompensa para adulterar, modificar u ocultar información conducente a un hallazgo evidenciado durante la auditoría, seguimiento o evaluación.

Tipo de Riesgo	**Seguridad de la Información**
Tipo de Activo	Datos Información Actas, informes de auditoría y seguimiento, Plan Anual de Auditoria
Riesgo.	Posibilidad de pérdida de Integridad por fallas humanas; de actas, informes de auditoría y seguimiento, PAA,
Causa	Debido a manejo manual de la información,
Objetivo de Control 1.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Control	El jefe de la Oficina de Control Interno verifica que los servidores de la Oficina pasen por los procesos de inducción y reinducción que le sean programados.
Objetivo de Control 2.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
Control	Cuando se presenten incidentes de integridad, el jefe de la Oficina de Control Interno revisa con su equipo de trabajo y con el oficial de seguridad el cumplimiento de la política de seguridad de la información al interior de la OCI.

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presenta niveles de criticidad baja, Se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo se debe gestionar dichos riesgos. Por otra parte, no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, no se detalla que pasa si el control falla. En la descripción del segundo control se evidencian una periodicidad de cuando se presenten incidentes de integralidad y para el primer control no determina la periodicidad, sin embargo, en la matriz hace referencia a una frecuencia con la que se realiza la actividad como permanente. No se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación.

4.3.8 PROCESO GESTIÓN DE RECURSOS FINANCIEROS A-CA-001

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Dirección Financiera
Nuevo Proceso	A-CA-010 GESTIÓN FINANCIERA
Objetivo del Proceso	Gestionar de manera eficiente y oportuna los recursos financieros de las diferentes fuentes de financiación a través de la programación, seguimiento a la ejecución presupuestal, programación de PAC, ordenación de pagos, cierre presupuestal y demás actividades de apoyo, en el marco de los principios y normas vigentes reflejándose en los Estados Financieros, con el fin de contribuir al cumplimiento de los objetivos institucionales

Tipo de Riesgo	**Gestión**
Riesgo	Posibilidad de afectación económica y reputacional por hallazgos administrativos, disciplinarios y penales y sanciones por entes de control.
Causas	Estados financieros con salvedades, interpretación errónea de la normatividad contable y falta de oportunidad, utilidad y confiabilidad en la información entregada por los proveedores de la misma.
Riesgo	Posibilidad de afectación económica y reputacional por hallazgos administrativos, disciplinarios y penales y sanciones por entes de control,
Causas	Inexactitud en los movimientos presupuestales (modificaciones, certificados de disponibilidad presupuestal, registros presupuestales, anulaciones)

Conclusiones: Se recomienda establecer nuevos riesgos conforme a los hallazgos administrativos contemplados en el Informe de Auditoría de Regularidad de la Contraloría de Bogotá con presunta incidencia disciplinaria por no presentar en el primer pago, el soporte de pago al Sistema de Seguridad Social y ARL y por falta de reporte e Inconsistencias en la información al momento de la rendición de cuenta de la SDP en el aplicativo SIVICOF.

Por otra parte, se pueden contemplar o establecer riesgos y controles por cambios normativos que afecten la ejecución del proceso, fallas tecnológicas de los aplicativos, posibilidad de generar información inconsistente o inoportuna, entre otros que afecten el cumplimiento de objetivos. Finalmente, no se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia soportada llegar a la misma conclusión.

Tipo de Riesgo	**Corrupción**
Riesgos	Posibilidad de aplicación incorrecta de la normatividad tributaria en el proceso de revisión y liquidación de pagos para favorecer a terceros
Causas	1. Interpretación errónea de la normatividad tributaria. 2. Presiones internas y/o externas para realizar la liquidación de pagos con el fin de favorecer a terceros.

Conclusiones: Se recomienda verificar y analizar nuevos riesgos que contemplen por ejemplo: Inclusión de gastos no autorizados, Favorecimiento indebido a terceros para la Administración de recursos públicos entre otros, por otra parte, se sugiere fortalecer el plan de acción contemplado para la vigencia 2024 para el tratamiento del riesgo que realmente mitigue dicho riesgo y que

ataque las causas originadoras del riesgo y no solo realizar capacitaciones de la nueva herramienta en SICAPITAL para procesar los certificados de cumplimiento y generar el archivo plano para subirlo a aplicativo Bogdata. Si es necesario realizar mesas de trabajo con el equipo de cuentas la Dirección Financiera indicando la periodicidad o cantidad de capacitaciones que se van a realizar que realmente mitiguen o reduzcan el riesgo.

Tipo de Riesgo	Seguridad de la Información
Tipo de Activo	Datos Información Instrumentos de apoyo no oficiales, para el cumplimiento de los objetivos del proceso, almacenados en los repositorios oficiales de la entidad.
Riesgo.	Posibilidad de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios de los instrumentos de apoyo no oficiales almacenados en los repositorios oficiales de la entidad, para el cumplimiento de los objetivos del proceso.
Causa	Debido a desconocimiento o no aplicación de las políticas de seguridad y privacidad, manejo manual de los archivos y deficiencia en la autorización de permisos de la información.
Objetivo de Control 1.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	El oficial de seguridad de la información de la entidad define, revisa, actualiza y socializa cada año las políticas de seguridad de la información y buenas prácticas del manejo de la información de la entidad.
Objetivo de Control 2.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
Control	El servidor de proceso diligencia el A-FO-010 en cada cambio de usuario, ya sea por ingreso o retiro del servidor y envía a la Dirección de Tecnologías de la Información y las Comunicaciones

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presenta niveles de criticidad BAJA, Se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo se debe gestionar dichos riesgos. Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, delimitar el responsable del control para el caso del *proceso Soporte Tecnológico* es importante establecer el cargo (profesional, técnico, coordinador o jefe) que realiza no se puede generalizar y detallar qué pasa si el control falla.

Por otra parte, en la descripción del control se evidencian frecuencias semestrales, periódicas y en otras no determina la periodicidad, sin embargo, en la matriz hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Atender lo indicado en el *Informe de Auditoría de Sistemas de Gestión* de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

4.3.9 PROCESO GESTIÓN DOCUMENTAL A-CA-002

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano,

	simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Dirección Administrativa.
Proceso Nuevo	A-CA-012 GESTIÓN ADMINISTRATIVA
Objetivo del Proceso	Preservar el patrimonio documental de la SDP, mediante la administración, custodia y conservación de la documentación del archivo y publicaciones, para asegurar la información como un activo institucional y un derecho de la comunidad

Tipo de Riesgo	Gestión
Riesgos	Posibilidad de afectación económica y reputacional por pérdida o deterioro de documentos de archivo.
Causas	Falencias en el diseño, despliegue e implementación de Políticas de Gestión Documental

Conclusiones: Se sugiere analizar la identificación de nuevos riesgos no solo por perdida o deterioro de documentos como pueden ser: las consecuencias por administrar en forma inadecuada el ciclo vital de los documentos, aplicar de forma inadecuada los instrumentos archivísticos por cambios para su adecuada aplicación. Finalmente, en los controles identificados no se registra la evidencia de la ejecución del control y donde quedan almacenados.

Tipo de Riesgo	Corrupción
Riesgos	Posibilidad de adulteración o sustracción de la documentación custodiada por la Dirección Administrativa con participación de servidores y/o contratistas de la entidad
Causas	1. No acatamiento de las políticas, procedimientos y directrices de gestión documental, por parte de los funcionarios de la SDP 2. Falta de conocimiento, por parte de usuarios internos y externos, de los requisitos y condiciones para ser usuario de los servicios documentales de la SDP. 3. Documentación sin la completa intervención documental.

Conclusiones: Se sugiere analizar la identificación de nuevos riesgos y controles teniendo en cuenta la entregar información a terceros violando los acuerdos de confidencialidad y los lineamientos establecidos en la entidad, buscando un beneficio particular. Por otra parte, se debe registrar el responsable del control estableciendo el cargo (profesional, técnico, coordinador o jefe) que realiza o ejecuta la actividad no se puede generalizar con los servidores de la dirección administrativa, y finalmente, no se registra la evidencia de la ejecución del control y donde quedan almacenados.

Tipo de Riesgo	Seguridad de la Información
Tipo de Activo	Datos Información Información que se encuentra en diferentes medios removibles y que es identificada para preservar digitalmente.
Riesgo	Posibilidad de pérdida de disponibilidad por destrucción de la información, que se encuentra en diferentes medios removibles y que es identificada para preservar digitalmente.
Causa	Debido a copias insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información, copias no controladas, información sensible sin cifrado, ausencia de copias de respaldo o backup de la información
Objetivo de Control 1.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.

Control	Todos los servidores públicos, contratistas, pasantes de la SDP aplican de forma permanente lo establecido en la Política de uso de medios removibles A-LE-320 en cuanto a la seguridad de la información.
Objetivo de Control 2.	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
Control	Todos los servidores públicos, contratistas, pasantes de la SDP aplican de forma permanente lo establecido en la Política de gestión de activos de información A-LE-474
Objetivo de Control 3.	Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
Control	Todos los funcionarios y contratistas de la SDP aplican de forma permanente lo establecido en la Política de uso de medios removibles A-LE-320 en cuanto a la transferencia de información y el Plan de Preservación Digital a Largo Plazo A-LE-438.
Objetivo de Control 4.	Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
Control	Todos los servidores públicos, contratistas, pasantes de la SDP organizan y clasifican los expedientes electrónicos de archivo según lo establecido en las TRD y lineamientos impartidos
Riesgo	Posibilidad de pérdida de disponibilidad por mal funcionamiento del software; utilizado para la visualización de la información susceptible para preservar digitalmente (word, excel, ppt, tiff...), por mal funcionamiento del software y saturación del sistema de información,
Causa	Debido a ausencia de la gestión en el versionamiento de los sistemas de información, software nuevo o inmaduro o ausencia de mecanismos de identificación y autenticación en los sistemas de información.
Objetivo de Control 1.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define el Procedimiento de Instalación y administración de software A-PD-198 velando por su correcta aplicación.
Objetivo de Control 2.	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define la Política de uso de Software A-LE-362, el procedimiento de valoración de aplicaciones de software y/o sistemas de información A-PD-166.
Objetivo de Control 3.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	La Dirección Administrativa define el Plan de Preservación Digital a Largo Plazo A-LE-438. La Dirección de Tecnologías de la Información y las Comunicaciones define la política de seguridad y privacidad de la información A-LE-429.
Objetivo de Control 4.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define la política para la gestión de copias de respaldo y recuperación de la información institucional A-LE-297 y aplica el procedimiento de copias de seguridad y recuperación de información A-PD-092
Riesgo 3.	Posibilidad de Perdida de Disponibilidad por mal funcionamiento del software que afecte la información almacenada en SGDEA o en el módulo de preservación digital, debido a software nuevo o inmaduro, configuración incorrecta de parámetros , ausencia de la gestión en el versionamiento de los sistemas de información, ausencia de control de cambios en sistemas de información además por Error en el uso o abuso de derechos y

	privilegios debido a la Gestión deficiente de las contraseñas - Contraseñas sin protección y por la Falsificación de derechos de acceso de información
Causa	Debido a la Ausencia de mecanismo de identificación y autenticación en los sistemas
Objetivo de Control 1.	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define aplica y hace seguimiento a la Política de Control de Acceso A-LE- 315
Objetivo de Control 2.	Se debe restringir el acceso a los códigos fuente de los programas.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define aplica y realiza seguimiento a la política de Desarrollo Seguro A-LE-359 y Política de Control de Acceso A-LE- 315
Objetivo de Control 3.	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define aplica y realiza seguimiento a la implementación de las directrices generales para la formulación de proyectos informáticos A-LE-285
Objetivo de Control 4.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define aplica y realiza seguimiento al modelo de seguridad y privacidad de la información de la SDP, adicional a esto el oficial de seguridad de la información realiza de manera constante campañas de sensibilización frente al buen manejo de las contraseñas
Objetivo de Control 5.	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones realiza jornadas de depuración de usuarios a los sistemas de información
Riesgo 4.	Posibilidad de Perdida de Disponibilidad por mal funcionamiento del equipo de cómputo o servidores que almacenan la información a preservar digitalmente, debido a ausencia de esquemas de reemplazo periódico, por fallas del equipo
Causa	Debido a la obsolescencia tecnológica tipo hardware y por uso no autorizado del equipo por el Acceso al Hardware sin protección o protocolos de seguridad
Objetivo de Control 1.	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define aplica y realiza seguimiento a la implementación del Plan de Mantenimiento de infraestructura tecnológica de la SDP A-LE-389 y el Plan Estratégico de Tecnología de la Información
Objetivo de Control 2.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones define aplica y realiza seguimiento a la implementación del Plan de Mantenimiento de infraestructura tecnológica de la SDP A-LE-389
Riesgo 5.	Posibilidad de pérdida de disponibilidad, en lugar de almacenamiento de los equipos, medios removibles, o servidores donde se almacena la información a preservar digitalmente; por fenómenos climáticos, fuego, agua o fenómenos sísmicos;
Causa	Debido a ausencia de mecanismos de dispersión de humo y fuego, uso inadecuado de los controles de acceso físico a las edificaciones y áreas seguras, ubicación en un área susceptible de inundación, ausencia de protección física de la edificación, puertas y ventanas.

Objetivo de Control 1.	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones y la Dirección Administrativa define aplica y realiza seguimiento a la implementación de la Política de seguridad física y del entorno A-LE 452
Objetivo de Control 2.	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
Control	La Dirección Administrativa supervisa el cumplimiento y ejecución del contrato de vigilancia cuyo objeto es prestar los servicios de la vigilancia y seguridad privada en la modalidad de vigilancia fija, para las instalaciones y bienes muebles de la SDP, así como aquellos por los cuales sea o llagare a ser legalmente responsable
Objetivo de Control 3.	Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
Control	La Dirección de Tecnologías de la Información y las Comunicaciones y la Dirección Administrativa define aplica y realiza seguimiento al cumplimiento de las condiciones de seguridad y de protección contra amenazas externas y ambientales en el Data Center principal de la SDP
Riesgo 6.	Posibilidad de Perdida de Disponibilidad por fallas humanas; de personas responsables de la producción, gestión, almacenamiento y custodia de la información a preservar digitalmente.
Causa	Debido a insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información.
Objetivo de Control 1.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Control	La Dirección Administrativa realiza la implementación del Programa de Cualificación en Gestión Documental establecido para cada vigencia y el oficial de seguridad de la información realiza de manera constante campañas de sensibilización frente al buen manejo de las contraseñas y la Política de Seguridad de la Información
Objetivo de Control 2.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	La Dirección Administrativa y la Dirección de Tecnologías de la Información y las Comunicaciones de manera constante realizan campañas de buenas prácticas y socialización de políticas del uso aceptable de los activos de información
Objetivo de Control 3.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
Control	La Dirección Administrativa y la Dirección de Tecnologías de la Información y las Comunicaciones realizan seguimiento al cumplimiento de las Políticas establecidas en el Sistema de Gestión de Seguridad de la Información y a la Política de Gestión Documental

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presenta niveles de criticidad Baja y Media, por lo que se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo se debe gestionar dichos riesgos. Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, delimitar el responsable del control para el caso del *proceso Soporte Tecnológico* es importante establecer el cargo (profesional,

técnico, coordinador o jefe) que realiza no se puede generalizar y detallar qué pasa si el control falla.

Por otra parte, en la descripción del control se evidencian frecuencias semestrales, periódicas y en otras no determina la periodicidad, sin embargo, en la matriz hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Finalmente, en los planes de acción para el tratamiento de reducir o mitigar el riesgo teniendo en cuenta la zona de riesgo residual Extrema, deben contar con un indicador clave de riesgo que le permita capturar la ocurrencia de un incidente que se asocia al riesgo identificado previamente.

4.3.10 PROCESO MEJORAMIENTO CONTINUO - S-CA-002

Objetivo Estratégico	4. Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	Dirección de Planeación Institucional
Proceso Nuevo	E-CA-004 DIRECCIÓN ESTRATÉGICA INSTITUCIONAL
Objetivo del Proceso nuevo	Direccionar la formulación, ejecución, seguimiento y actualización de la planeación institucional a nivel estratégico, táctico y operativo mediante la definición e implementación de lineamientos e instrumentos de planeación, que permitan lograr el cumplimiento de la misión, visión y compromisos del plan distrital de desarrollo, facilitando la toma de decisiones, contribuyendo a la mejora continua y generando valor público.
Objetivo del Proceso anterior	Fortalecer la gestión de la Secretaría Distrital de Planeación mediante la mejora del desempeño de los procesos, productos y servicios, para aumentar la capacidad institucional, prevenir o reducir efectos no deseados y contribuir a la mejora en la prestación del servicio.

Tipo de Riesgo	**Gestión**
Riesgo	Posibilidad de afectación económica y reputacional por sanciones y/o multas por parte de órganos de control, requerimientos de grupos de valor y grupos de interés y/o pérdida de confianza y credibilidad, debido a debilidad en:
Causas	1. Apropiación de los principios de autocontrol, autogestión y autorregulación en las líneas de defensa (estratégica, primera, segunda y tercera línea) 2. En la formulación, ejecución, reporte, monitoreo y seguimiento de los planes de mejoramiento.
Controles	1. El Subsecretario(a), Director(a), Subdirector(a), Jefe de Oficina que actúa como responsable del plan de mejoramiento conjuntamente con su equipo de trabajo, cada vez que se vaya a formular un plan, verifica que este se formule en términos de oportunidad y pertinencia, conforme con lo establecido en el procedimiento S-PD-005 Gestión del Plan de Mejoramiento. Las observaciones, ajustes o novedades serán consignadas en el documento soporte de la reunión del equipo de trabajo. 2. El profesional de la Dirección de Planeación Institucional verifica metodológicamente que el Plan de Mejoramiento guarde coherencia entre las causas y acciones frente a los hallazgos, que las acciones hayan sido formuladas en el marco del PHVA, que los plazos de las acciones sean coherentes, revisa la viabilidad de las homologaciones, coherencia de metas e indicadores y el completo diligenciamiento de los campos del módulo de planes de mejoramiento del sistema dispuesto por la entidad. Las observaciones quedan registradas en dicho módulo. 3. El Subsecretario(a), Director(a), Subdirector(a), Jefe de Oficina que actúa como responsable del plan de mejoramiento y su equipo de trabajo verifican mensualmente

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por sanciones y/o multas por parte de órganos de control, requerimientos de grupos de valor y grupos de interés y/o pérdida de confianza y credibilidad, debido a debilidad en:
	el estado de avance de las acciones definidas en dichos planes y las evidencias que dan cuenta de la gestión realizada, así como las observaciones efectuadas por parte de la Oficina de Control Interno, si las hay. Las observaciones, ajustes o novedades serán consignadas en el módulo de planes de mejoramiento del sistema de seguimiento dispuesto por la entidad.

Conclusiones: La Oficina de Control Interno en el *Informe de seguimiento a la gestión de los planes de mejoramiento del 1 de julio al 30 de septiembre de 2023*, estableció la situación crítica 2179 *"Se evidencian acciones de mejora que carecen de efectividad, en atención a que no se ha logrado subsanar los hallazgos y situaciones críticas identificados en diferentes ejercicios auditores realizados tanto por entidades externas como por fuentes internas, relacionados con Peticiones, Quejas, Reclamos y Sugerencias PQRS relacionados entre otros con vencimiento de términos, debilidades en los aplicativos utilizados y en los reportes generados.",* relacionada con la efectividad de acciones de planes de mejoramiento, denotando una posible materialización del riesgo, sin que el *Informe monitoreo de segunda línea de defensa a los mapas de riesgos de gestión, corrupción y de seguridad de la información de la secretaría distrital de planeación a diciembre de 2023*, lo haya manifestado: *"Con corte al mes de diciembre de 2023 no se cuenta con hallazgos de auditoría asociados a los controles identificados en el mapa de riesgos del proceso."*

Adicional a lo anterior, en el Informe de Auditoría de Sistemas de Gestión vigencia 2023, Icontec estableció una oportunidad de mejora respecto a planes de mejoramiento *"Cuando se formulan planes de mejora para resolver los hallazgos reportados por auditorías y evaluaciones internas, es necesario asegurar que las correcciones eliminan de fondo el hallazgo reportado. Dichas acciones deben estar enfocadas en adoptar medidas para superar la deficiencia reportada y que las evidencias y sus resultados así lo demuestren (enfoque en el resultado, no en el medio)."*

Adicionalmente, se sugiere revisar la necesidad de tener en cuenta lo relacionado con el incumplimiento de los planes de mejoramiento, atendiendo lo establecido en la Resolución Reglamentaria 036 de 2023 de la Contraloría de Bogotá, *"Por la cual se modifica y reglamenta el trámite del Plan de Mejoramiento que presentan los sujetos de vigilancia y control a la gestión fiscal de Contraloría de Bogotá D.C. y se adopta el procedimiento interno"* en cuanto a las sanciones que implica el incumplimiento de los términos establecidos en los planes de mejoramiento. Por otra parte, los controles se encuentran asociados a la segunda causa raíz, por lo que se sugiere analizar a fin de determinas si es necesario incluir controles al respecto.

Tipo de Riesgo	Información
Activo de Información	Datos Información. Documentos históricos de consulta y soporte (actas, resoluciones, procedimientos, planes)
Riesgo	Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información, contenida en documentos históricos de consulta y soportes (actas, resoluciones, planes) debido a:
Causas	1. Fallas humanas y destrucción de la información, contenida en documentos históricos de consulta y soportes (actas, resoluciones, planes) debido a 2. manejo manual de la información 3. insuficiente entrenamiento y capacitación sobre políticas y privacidad de la información.

Tipo de Riesgo	Información
Activo de Información	Datos Información. Documentos históricos de consulta y soporte (actas, resoluciones, procedimientos, planes)
Riesgo	Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información, contenida en documentos históricos de consulta y soportes (actas, resoluciones, planes) debido a:
Objetivo de Control 1	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control 1	El Líder de seguridad de la información define y divulga las políticas de seguridad y del buen tratamiento, uso y custodia de la información por parte de los diferentes colaboradores de la entidad.
Objetivo de Control 2	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
Control 2	La empresa que presta el servicio de seguridad física valida la identidad de quien solicita el acceso a las instalaciones. Para el caso de los funcionarios registra la información en la bitácora, si es visitante solicita la autorización de acceso.
Objetivo de Control 3	Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
Control 3	Se cuenta con un archivador metálico para el almacenamiento de los documentos históricos.

Conclusiones: El activo de información no se encuentra definido en concordancia con el A-LE-283 *Registro De Activos De Información* (RAI). Se sugiere el fortalecimiento de los controles atendiendo las características de un control (responsable, periodicidad, propósito, evidencia) definidas en la *E-LE-030 Política de administración del riesgo* y la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* en su versión 4, a fin de salvaguardar la integridad de los activos, atendiendo tanto el activo en su forma digital como física. Lo anterior, atendiendo a que contar con un archivador no puede considerarse un control, ni tampoco la divulgación de las políticas, siendo importante complementarlo con los elementos necesarios para la conservación documental.

Adicionalmente, se recomienda la revisión del *M-LE-223 Mapa de Riesgos de Seguridad de la Información del Proceso Coordinación de las Políticas Públicas y de los Instrumentos de Planeación*, a fin de que muestre la *Evaluación del Riesgo - Nivel del Riesgo Residual* por riesgo y no por cada control como está apareciendo actualmente.

Tipo de Riesgo	Información
Activo de Información	Datos Información. Planes de Mejoramiento
Riesgo	Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información, contenida en documentos históricos de consulta y soportes (actas, resoluciones, planes) debido a:
Causas	1. Fallas humanas y destrucción de la información, contenida en documentos históricos de consulta y soportes (actas, resoluciones, planes) debido a 2. manejo manual de la información 3. insuficiente entrenamiento y capacitación sobre políticas y privacidad de la información. 4. ausencia de copias de respaldo o backup de la información.

Tipo de Riesgo	**Información**
Activo de Información	Datos Información. Planes de Mejoramiento
Riesgo	Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información, contenida en documentos históricos de consulta y soportes (actas, resoluciones, planes) debido a:
Objetivo de Control 1	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes
Control 1	El Líder de seguridad de la información define y divulga las políticas de seguridad y del buen tratamiento, uso y custodia de la información por parte de los diferentes colaboradores de la entidad.
Objetivo de Control 2	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control 2	La Dirección de Tecnologías de la Información y las Comunicaciones realiza de forma periódica las copias de respaldo de los sistemas de información, bases de datos y de las carpetas compartidas, así como la restauración de las mismas.

Conclusiones: El activo de información no se encuentra definido en el A-LE-283 *Registro de Activos de Información* (RAI). Se sugiere que para mayor claridad se defina un riesgo referente al manejo de información física y otro para el tema digital, a fin de poder establecer controles más enfocados a la causa raíz que los origina. Igualmente, fortalecer los controles atendiendo las características de un control (responsable, periodicidad, propósito, evidencia) definidas en la *E-LE-030 Política de administración del riesgo* y la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* en su versión 4, a fin de salvaguardar la integridad de los activos, atendiendo tanto el activo en su forma digital como física. Adicionalmente, se recomienda la revisión del *M-LE-223 Mapa de Riesgos de Seguridad de la Información del Proceso Coordinación de las Políticas Públicas y de los Instrumentos de Planeación*, a fin de que muestre la *Evaluación del Riesgo - Nivel del Riesgo Residual* por riesgo y no por cada control como está apareciendo actualmente.

Tipo de Riesgo	**Corrupción**
Riesgo	Posibilidad de manipulación de la información relacionada con las acciones de los planes de mejoramiento, por acción u omisión con el fin de desviar la gestión en beneficio propio o de terceros
Causas	1. Vacíos en el cumplimiento del procedimiento para la formulación y reformulación de las acciones de los planes de mejoramiento. 2. Presiones de funcionarios con poder de decisión para ajustar o modificar acciones de los planes de mejoramiento.
Controles	1. El (Subsecretario(a), Director(a), Subdirector(a) o Jefe de Oficina responsable del Plan de Mejoramiento y el Profesional Especializado y/o Universitario con rol de enlace SG-MIPG verifican cada vez que se requiera, los avances de las acciones de los planes de mejoramiento a su cargo con el fin de establecer el estado de las mismas al momento de reportar el monitoreo de primera línea de defensa en el módulo Planes de Mejoramiento del SIPA, de acuerdo con los plazos establecidos para tal fin. Como insumo consultan los informes de seguimiento a planes de mejoramiento elaborados por la OCI. Si encuentran alguna observación, ajuste o novedad, la reporta en el monitoreo correspondiente.

Tipo de Riesgo	**Corrupción**
Riesgo	Posibilidad de manipulación de la información relacionada con las acciones de los planes de mejoramiento, por acción u omisión con el fin de desviar la gestión en beneficio propio o de terceros
	2. El profesional especializado y/o universitario y el Jefe de Oficina de Control Interno trimestralmente verifican el estado de avance de las acciones de los planes de mejoramiento (en desarrollo, en alerta, vencida, cumplimiento en seguimiento, en seguimiento y cerrada) y lo registran en SIPA , así mismo, validan que las evidencias cargadas por las dependencias en el repositorio definido por la entidad para tal fin, sean claras, objetivas y suficientes para determinar la gestión realizada y el estado de las acciones. Las observaciones, ajustes o novedades las registran en SIPA.

Conclusiones: Se sugiere la revisión atendiendo a que las causas raíz están orientadas a formulación, reformulación y ajuste, mientras que los controles hacia los avances y seguimientos. Adicionalmente, no se identifican acciones relacionadas con las actividades a cargo de la Dirección de Planeación Institucional como segunda línea de defensa, en todas las etapas del plan de mejoramiento.

4.3.11 PROCESO PARTICIPACIÓN Y COMUNICACIÓN E-CA-003

Objetivos Estratégicos	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
	Diseñar y generar espacios colaborativos de participación ciudadana con enfoque diferencial, en la formulación, seguimiento y evaluación de los instrumentos y procesos de planeación.
Líder Proceso	OFICINA DE PARTICIPACIÓN Y DIALOGO DE CIUDAD
Proceso	Nuevos: E-CA-005 COMUNICACIÓN ESTRATÉGICA E-CA-008 ARTICULACIÓN DEL DIÁLOGO CON EL CIUDADANO E-CA-009 ARTICULACIÓN DEL DIÁLOGO CON LAS INSTITUCIONES
Objetivo del Proceso	Elaborar e implementar estrategias de participación y comunicación internas y externas de acuerdo a los lineamientos establecidos por la Administración Distrital, para posicionar a la SDP y fortalecer las decisiones de la planificación del desarrollo integral de la ciudad.

Tipo de Riesgo	**Gestión**
Riesgo	Posibilidad de afectación económica y reputacional por incumplimiento de los lineamientos contenidos en el modelo colaborativo de participación que se sustenta en los pilares de gobierno abierto (transparencia, rendición de cuentas, participación y colaboración)
Causas	Inadecuado diseño y/o implementación, seguimiento y evaluación de las estrategias de participación para la formulación de los instrumentos de planeación
Control 3	El líder del Proceso de Participación y Comunicación verifica, cada vez que se implementa una estrategia de participación para un instrumento de planeación, que dicha estrategia se encuentre alineada con los criterios de contenido y estructura definidos en el procedimiento E-PD-020 Diseño e implementación de las estrategias de participación ciudadana en los instrumentos de planeación de la SDP.
Riesgos	Posibilidad de afectación reputacional por entrega de información incompleta, errónea, inoportuna o confusa,

Tipo de Riesgo	Gestión
Causas	La desarticulación de las áreas de la SDP con la Oficina Asesora de Comunicaciones, la variación de los tiempos para la generación de la información por factores exógenos, la divulgación de información a los medios de comunicación por parte de funcionarios públicos y contratistas sin autorización
Control 4	El/la profesional de la Oficina de Comunicaciones encargado, verifica cada vez que se realiza un producto de comunicaciones, este cumpla con los criterios definidos en el procedimiento E-PD-015 Gestión para la conceptualización y elaboración de los productos de comunicación.

Conclusiones: Se sugiere revisar la identificación de nuevos riesgos, causas y controles o fortalecer los ya existentes, contemplando los hallazgos realizados en los informes de auditoría tanto internas (Informe de auditoría al Sistema de Gestión de la Calidad en la vigencia 2021.) como externas (INFORME FINAL DE AUDITORIA DE REGULARIDAD Código de Auditoría No. 51 Fecha: abril de 2021, PAD 2021 Vigencia 2020, Hallazgo administrativo con incidencia fiscal y presunta incidencia disciplinaria, por mayores valores pagados, pagos de productos sin soportes y por el pago de ítems no previstos que no cuentan con los soportes que sustenten el recibo a satisfacción por parte de la SDP). Finalmente, en los controles identificados no se registra la evidencia de la ejecución del control y donde quedan almacenados.

Se recomienda la revisión del tercer control correspondiente al primer riesgo y del cuarto control del segundo riesgo, ya que fueron catalogados como correctivos, sin que se relacionara con la gestión en el evento de una materialización de riesgos.

Tipo de Riesgo	Corrupción
Riesgos	Posibilidad de manipulación de los instrumentos de planeación en los procesos de participación ciudadana con el fin de obtener el beneficio propio o de un tercero.
Causas	1. Existencia de intereses particulares en la formulación de un determinado instrumento de planeación. 2. Desconocimiento de las normas que rigen la participación ciudadana en los instrumentos de planeación. 3. Desconocimiento de los lineamientos de participación impartidos por la Secretaría de Planeación. 4. Desconocimiento de las políticas de seguridad de la información de la Secretaría de Planeación. 5. Desconocimiento del Código de Ética y Código General Disciplinario.

Conclusiones: Teniendo en cuenta el plan de acción para la vigencia 2024, "Socializar a los servidores públicos y demás colaboradores de la dependencia, en temas relacionados con Código General Disciplinario, Código de Ética y gestión de los riesgos asociados al proceso", para el tratamiento del riesgo se debe establecer la periodicidad con la que se realizaran estas socializaciones y la fecha de seguimiento con sus evidencias. Atender lo indicado en el *Informe de Auditoría de Sistemas de Gestión* de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

Tipo de Riesgo	**Seguridad de la Información**
Tipo de Activo	Datos Información Bases de datos, evidencias de los procesos de participación y comunicación, insumos para la divulgación de información y documentos de gestión administrativa y misional
Riesgo 1.	Posibilidad de Pérdida de Disponibilidad por fallas humanas, fallas del equipo, destrucción de la información, hurto de la información y saturación del sistema de información, de las bases de datos, evidencias de los procesos de participación y comunicación y documentos de gestión administrativa y misional,
Causa	Debido a desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, ausencia de copias de respaldo o backup de la información, deficiencia en la autorización de permisos de la información, ausencia o deficiencia en los sistemas de autenticación de los aplicativos.
Objetivo de Control 1.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican que cada año se realicen capacitaciones relacionadas con la aplicación de las políticas de seguridad y privacidad de la información.
Objetivo de Control 2.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican que cada año se socialicen las políticas de seguridad de la información.
Objetivo de Control 3.	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican que, permanentemente, se apliquen los procedimientos para asignar y revocar los derechos de acceso a los usuarios para todos los sistemas y servicios.
Objetivo de Control 4.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican que, permanentemente, sé realice mantenimiento preventivo a los equipos para asegurar su correcto funcionamiento.
Objetivo de Control 5.	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican que se realicen, periódicamente una revisión de la ubicación de los equipos y acceso seguro a la información para evitar fuga de información y perdida de confidencialidad.
Riesgo 2.	Posibilidad de Pérdida de Confidencialidad por fallas humanas, uso no autorizado del equipo, copia fraudulenta del software, hurto de Información de bases de datos, evidencias de los procesos de participación y comunicación, insumos para la divulgación de información y documentos de gestión administrativa y misional.
Causa	por desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, deficiencia en la autorización de permisos de la información, copias no controladas, ausencia de validación de autenticación de la información
Objetivo de Control 1.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

Tipo de Riesgo	Seguridad de la Información
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican, permanentemente, que el acceso a la información sea restringido, de acuerdo con la política de seguridad y privacidad de la información.
Objetivo de Control 2.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican que periódicamente las personas autorizadas realicen las capacitaciones en torno al cumplimiento del procesamiento y procedimientos del manejo de la información en el área.
Objetivo de Control 3.	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones verifican que se realicen, periódicamente una revisión de la ubicación de los equipos y acceso seguro a la información para evitar fuga de información y perdida de confidencialidad.
Objetivo de Control 4.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control	El/la Jefe de la Oficina de Participación y Diálogo de Ciudad y el/la Jefe de la Oficina Asesora de Comunicaciones solicitan anualmente a la Dirección de Sistemas que se realicen las copias de respaldo de la información de cada dependencia.

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presentan niveles de criticidad Media, teniendo en cuenta la Confidencialidad, disponibilidad e integralidad de la información por lo que se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo se debe gestionar dichos riesgos. Es importante atender lo indicado en el *Informe de Auditoría de Sistemas de Gestión* de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, no se detalla que pasa si el control falla. En la descripción del control se evidencian frecuencias anuales, periódicas y en otras no determina la periodicidad sin embargo en la matriz de riesgos, hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Por otra parte, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación.

Finalmente, para el primer objetivo de control no se registra plan de acción para la vigencia 2024 en el mapa de riesgos teniendo en cuenta la zona de riesgo final como ALTO conforme a los niveles de aceptación del riesgo y su tratamiento establecidos en la política de administración de riesgos.

4.3.12 PLAN DE ORDENAMIENTO TERRITORIAL (POT) - M-CA-005

Objetivo Estratégico	2. Definir y promover un modelo colectivo de ciudad en el largo plazo, mediante la reglamentación y viabilización del territorio, a través de los instrumentos de planeación buscando el bienestar de la ciudadanía.
Líder Proceso	Subsecretaria de Planeación Territorial
Proceso Nuevo	Planeación Territorial y Gestión de sus Instrumentos - M-CA-001
Objetivo Proceso	Generar un modelo de ordenamiento territorial acorde con las necesidades distritales mediante la formulación del plan de ordenamiento territorial y las Acciones Urbanísticas, Actuaciones Administrativas y Formulación de Proyectos Distritales que lo implementan, con el fin de facilitar el desarrollo urbano y rural en términos de equilibrio y equidad territorial para el beneficio social.

Tipo de Riesgo	**Gestión**
Riesgo	Posibilidad de afectación económica y reputacional por decisiones jurídicas en contra de las acciones relacionadas con el ordenamiento territorial debido a:
Causas	1. Seguimiento y evaluación inadecuadas frente a la implementación del Plan de Ordenamiento Territorial - POT vigente antes de la adopción del nuevo POT; 2. Insuficiencia y falta de acceso a datos, información y estudios poblacionales y del territorio para un adecuado diagnóstico del modelo de ordenamiento territorial; 3. Documentos del POT sin los contenidos mínimos establecidos en las normas vigentes; 4. Incumplimiento en las etapas de planificación territorial definidas por la ley y fallas en el proceso de formulación del POT con las partes interesadas (concertación, consulta, aprobación y adopción).
Controles	1. El(la) Subsecretario(a) de Planeación Territorial verifica cada vez que se realiza una revisión al Plan de Ordenamiento Territorial - POT, que el seguimiento y evaluación del POT vigente y el diagnóstico del estado actual del territorio cumplan con los contenidos mínimos establecidos en la normatividad vigente; si los documentos y sus anexos no cumplen con los requisitos, se ajusta su contenido. 2. El(la) Subsecretario(a) de Planeación Territorial verifica cada vez que se realiza una revisión al Plan de Ordenamiento Territorial - POT, que la programación de las etapas definidas para su formulación cumpla con lo establecido en la normatividad vigente, si no cumple, se realizan los correspondientes ajustes a la programación. 3. El(la) Subsecretario(a) de Planeación Territorial verifica cada vez que se realiza una revisión al Plan de Ordenamiento Territorial - POT, que la totalidad de los documentos necesarios para la concertación ambiental cumpla con los contenidos mínimos establecidos en las normas vigentes; si el documento remisorio y sus anexos no cumplen con los requisitos, se ajusta su contenido. 4. La Subsecretaria de Planeación Territorial verifica cada vez que se realiza una revisión al Plan de Ordenamiento Territorial - POT, que la totalidad de los documentos necesarios para la consulta ante el Consejo Territorial de Planeación Distrital (CTPD) y Consejo Consultivo de Ordenamiento Territorial cumplan con los contenidos mínimos establecidos en las normas vigentes, en caso de que el documento remisorio y sus anexos no cumplan con los requisitos se ajusta su contenido. 5. El(la) Subsecretario(a) de Planeación Territorial verifica cada vez que se realiza una revisión al Plan de Ordenamiento Territorial - POT, que la totalidad de los documentos necesarios para su presentación ante el Concejo de Bogotá cumpla con los contenidos mínimos establecidos en las normas vigentes, en caso de que el documento remisorio y sus anexos no cumplan con los requisitos se ajusta su contenido.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por decisiones jurídicas en contra de las acciones relacionadas con el ordenamiento territorial debido a:
	6. El(la) Subsecretario(a) de Planeación Territorial en conjunto con la Subsecretaría Jurídica verifican al momento de recibir los resultados de una decisión judicial que suspenda de manera provisional o declare la nulidad del Plan de Ordenamiento Territorial - POT las implicaciones de esta decisión y las medidas que apliquen respecto a la normatividad vigente.

Conclusiones: Se sugiere mejorar la redacción del riesgo, atendiendo a que no es fácil su comprensión. Por otra parte, se recomienda el análisis de los controles y causas, dado que en su mayoría están referidos a la revisión del POT, desconociendo otras actuaciones relacionadas con el territorio que pueden materializar el riesgo.

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por entrega de los productos y/o servicios del proceso sin los requisitos de calidad establecidos como: claridad, legibilidad, oportunidad y legalidad, debido a:
Causas	1. Inconsistencias en la documentación técnica de soporte de los actos administrativos; 2. Desarticulación de los procesos de la Secretaría Distrital de Planeación en la generación de instrumentos de planeación territorial; 3. Falta de coordinación interinstitucional de las entidades que inciden en la planeación territorial; 4. Desconocimiento de los requerimientos de las partes interesadas en el proceso; 5. Desconocimiento previo del territorio para la proyección de los actos administrativos; 6. Desconocimiento por parte de la comunidad en el proceso de participación sobre la dinámica del mismo y la integralidad del proyecto; 7. Publicación inoportuna de los actos administrativos en los diferentes medios de publicación y desactualización de la información de la Base de Datos Geográfica Corporativa – BDGC."
Controles	1. Cada vez que se radica un trámite el Profesional Universitario y/o Especializado de la dirección o subdirección responsable verifica mediante lista de chequeo que los documentos para el inicio del trámite estén completos de acuerdo a los requerimientos establecidos en los procedimientos internos; si no se cumplen con los requisitos, se requiere formalmente al solicitante. 2. Cada vez que se radica un trámite el Profesional Universitario y/o Especializado de la dirección o subdirección responsable verifica que los documentos para el inicio de los trámites estén acordes con los requerimientos establecidos en la normatividad vigente; en caso de que no cumplan con los requisitos, se requiere al solicitante mediante oficio con requerimientos. 3. Cada vez que se proyecta un acto administrativo el director(a) y/o subdirector (a) de la Subsecretaría de Planeación Territorial revisa que su contenido jurídico y técnico cumpla con la normatividad vigente, registra su visto bueno y/o firma en el documento físico o electrónico. En caso de que no cumpla con las características de calidad, se devuelve al Profesional Universitario y/o Especializado que proyectó el acto administrativo para los ajustes pertinentes. 4. Durante el proceso de adopción del acto administrativo el director(a) y/o subdirector (a) de la Subsecretaría de Planeación Territorial responsable del trámite, verifica que se haya socializado a las partes interesadas la formulación del proyecto radicada por el gestor, con el fin de generar observaciones al mismo, las cuales quedan

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación económica y reputacional por entrega de los productos y/o servicios del proceso sin los requisitos de calidad establecidos como: claridad, legibilidad, oportunidad y legalidad, debido a:
	registradas en el acto administrativo. Si las observaciones proceden, se realizan los ajustes necesarios en el proyecto de acto administrativo. 5. El Profesional Universitario y/o Especializado de la dirección o subdirección de la Subsecretaría de Planeación Territorial verifica mensualmente a través del aplicativo SIPG las causas por las cuales la ejecución de las metas y actividades POA relacionadas con la reglamentación del Plan de Ordenamiento Territorial (POT) y la viabilización de hectáreas no está de acuerdo con lo programado e implementa las soluciones correspondientes. 6. El Profesional Universitario y/o Especializado de la dependencia de la Subsecretaría de Planeación Territorial si al diligenciar la matriz de actos administrativos detecta que no se ha publicado de manera oportuna un acto administrativo expedido, verifica la trazabilidad de la publicación (Gaceta de Urbanismo y Construcción, la página WEB de la entidad y la BDGC-SINUPOT) con el profesional Universitario y/o Especializado responsable del expediente para establecer las causas que originaron la situación. En caso de no estar publicado solicita su publicación. (causa 7)

Conclusiones: Se sugiere mejorar la redacción del riesgo, atendiendo a que no es fácil su comprensión. Adicionalmente, se recomienda la revisión de los controles, atendiendo a que se identifican 7 causas, sin que de las causas 2, 3, 4, 5 y 6 se identifique un control directamente relacionado, se hace especial énfasis por su importancia a las causas 2 y 3 relacionadas con desarticulación de los procesos de entidad y falta de coordinación interinstitucional.

Adicionalmente, no se observa relación directa con las causas definidas y el control 5, relacionado con seguimiento a cumplimiento de metas. Adicionalmente, se calificó como control correctivo, sin embargo, no se relaciona con la gestión en el evento de una materialización de riesgos. Por lo anterior, se recomienda la revisión y ajuste en la clasificación de este atributo.

Sin embargo, en el Informe de Auditoría de Regularidad de la Contraloría de Bogotá Secretaría Distrital de Planeación, Código de Auditoría No. 46 PAD 2023, se estableció el hallazgo *"3.2.1.1 Hallazgo administrativo por el incumplimiento del principio de planeación para la ejecución de la meta 10 del proyecto 7631, en la vigencia 2022."*. Por lo anterior, se considera necesario tener en cuenta este hallazgo en los ajustes que se realicen a los riesgos del proceso.

Así mismo, tener en cuenta lo indicado en el *Informe Monitoreo de Segunda Línea de Defensa a los Mapas de Riesgos de Gestión, Corrupción y de Seguridad de la Información de la Secretaría Distrital de Planeación,* con corte a agosto de 2023, donde se hizo mención que en el primer semestre de 2023, la encuesta de satisfacción de la Dirección de Trámites Administrativos Urbanísticos reflejó un bajo grado de satisfacción (70%) de los usuarios en el cumplimiento en el trámite de factibilidad o permiso para la instalación de Estaciones Radioeléctricas. Así las cosas, esta dirección implementó 2 acciones de mejora, las cuales finalizaron en octubre de 2023. Es importante, atender lo indicado en el *Informe de Auditoría de Sistemas de Gestión* de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

Tipo de Riesgo	Información
Activo de Información	Datos Información. Información que conforma la producción documental oficial del Proceso de Planeación Territorial y Gestión de sus Instrumentos (Decretos, resoluciones, cartografía, actas de concertación Ambiental).
Riesgo	Posibilidad de Perdida de Disponibilidad por fallas humanas; de información que conforma la producción documental oficial del proceso de planeación territorial y gestión de sus instrumentos (decretos, resoluciones, cartografía, actas de concertación ambiental)., debido a manejo manual de la información, insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información
Causas	1. Por fallas humanas; de información que conforma la producción documental oficial del proceso de planeación territorial y gestión de sus instrumentos (decretos, resoluciones, cartografía, actas de concertación ambiental). 2. Debido a manejo manual de la información, 3. Insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información.
Controles	1. El oficial de seguridad información de la Dirección de Tecnologías de la Información y las Comunicaciones imparte periódicamente capacitaciones de inducción en Seguridad de la información al personal del proceso. 2. El jefe inmediato de la dependencia correspondiente recibe y revisa los formatos A-FO-128 Entrega de bienes y documentos y el A-FO-191 Acta de entrega puesto de trabajo, en donde se hace entrega de activos de información y se hace transferencia de conocimiento. 3. El profesional de la Dirección de Tecnologías de la Información y las Comunicaciones realiza la revisión de los usuarios (funcionarios y contratistas activos) para verificar si las solicitudes corresponden a la base de datos de directorio activo de la Entidad. 4. La Dirección de Tecnologías de la Información y las Comunicaciones periódicamente realiza copias de respaldo de la información de las carpetas públicas y privadas y de las carpetas especiales.

Conclusiones: Se sugiere que el riesgo haga mención además de la criticidad respecto de disponibilidad, también a la integridad. Igualmente, se considera importante que se tenga en cuenta tanto la información manejada tanto en forma física como digital. El activo aquí incluido hace mención de un consolidado de activos de información, por lo que se sugiere la revisión en el A-LE-283 Registro de Activos de Información (RAI), dado que no todos pueden estar clasificados como altos. Por otra parte, para este riesgo se establecieron 4 controles: uno asociado al oficial de seguridad de la información, dos a la Dirección de Tecnologías de la Información y un último control asociado al jefe inmediato de la dependencia correspondiente. Por lo anterior, se sugiere la revisión de los controles a fin de incluir algunos asociados al área líder del proceso y que se refieran tanto al manejo de información física como digital. En cuanto al cuarto control, se recomienda la revisión de la forma cómo se hace seguimiento a su ejecución dado que está definido para todas las dependencias.

Por otra parte, se recomienda la revisión del A-LE-518 *Mapa de Riesgos de Seguridad de la Información del Proceso Administración del Talento Humano,* a fin de que muestre la *Evaluación del Riesgo - Nivel del Riesgo Residual* por riesgo y no por cada control como está apareciendo actualmente. Adicionalmente, se observan casillas en EVALUACIÓN DEL RIESGO - NIVEL DEL RIESGO RESIDUAL cuyo tratamiento es *Reducir* sin que se establezca el plan de acción respectivo.

Tipo de Riesgo	**Corrupción**
Riesgo	Posibilidad de generación de condiciones normativas en los instrumentos de planeación sin el lleno de requisitos para favorecer a un tercero.
Causas	1. Ofrecimiento de dádivas a los funcionarios que intervienen en la generación de las condiciones normativas. 2. Interés de un funcionario en obtener beneficios a cambio de modificar las condiciones normativas. 3. No declaración de conflictos de interés por parte de los funcionarios. 4. Falta de publicidad de los actos administrativos (Web - BDGC/SINUPOT-Gaceta de Urbanismo y Construcción). 5. Desactualización de la información de la Base de Datos Geográfica Corporativa – BDGC-SINUPOT.
Controles	1. Cada vez que se suscribe un acto administrativo el director(a) y/o subdirector (a) de la Subsecretaría de Planeación Territorial revisa que su contenido jurídico y técnico cumpla con la normatividad vigente, registra su visto bueno y/o firma en el documento físico o electrónico. En caso de que no cumpla con las características de calidad, se devuelve al Profesional Universitario y/o Especializado que proyectó el acto administrativo para los ajustes pertinentes. 2. Cada vez que se radica un trámite el Profesional Universitario y/o Especializado de la dirección o subdirección responsable verifica mediante lista de chequeo que los documentos para el inicio del trámite estén completos de acuerdo a los requerimientos establecidos en los procedimientos internos; si no se cumplen con los requisitos, se requiere formalmente al solicitante. 3. El Profesional Universitario y/o Especializado de la dependencia de la Subsecretaría de Planeación Territorial si al diligenciar la matriz de actos administrativos detecta que no se ha publicado de manera oportuna un acto administrativo expedido, verifica la trazabilidad de la publicación (Gaceta de Urbanismo y Construcción, la página WEB de la entidad y la BDGC-SINUPOT) con el profesional Universitario y/o Especializado responsable del expediente para establecer las causas que originaron la situación. En caso de no estar publicado solicita su publicación.

Tipo de Riesgo	**Corrupción**
Riesgo	Posibilidad de expedición de conceptos relacionados con la planeación territorial para favorecimiento indebido a un tercero.
Causas	1. Ofrecimiento de dádivas a los funcionarios que intervienen en la generación de conceptos técnicos. 2. Interés de un funcionario en obtener beneficios a cambio de expedir o modificar los conceptos técnicos. 3. No declaración de conflictos de interés por parte de los funcionarios. 4. Falta de divulgación de los actos administrativos (Web - BDGC/SINUPOT-Gaceta de Urbanismo y Construcción).
Controles	1. Cada vez que se suscribe un concepto técnico el director(a) y/o subdirector (a) de la Subsecretaría de Planeación Territorial revisa que su contenido jurídico y técnico cumpla con la normatividad vigente, registrando su visto bueno y/o firma en el documento físico o electrónico. En caso de que no cumpla con las características de calidad se devuelve al profesional Universitario y/o Especializado de la dirección y/o subdirección que proyecto el concepto para los ajustes pertinentes. 2. El Profesional Universitario y/o Especializado de la dependencia de la Subsecretaría de Planeación Territorial si al diligenciar la matriz de actos administrativos detecta que no se ha publicado de manera oportuna un acto administrativo expedido, verifica la trazabilidad de la publicación (Gaceta de Urbanismo y Construcción, la página WEB

Tipo de Riesgo	**Corrupción**
Riesgo	Posibilidad de expedición de conceptos relacionados con la planeación territorial para favorecimiento indebido a un tercero.
	de la entidad y la BDGC-SINUPOT) con el profesional Universitario y/o Especializado responsable del expediente para establecer las causas que originaron la situación. En caso de no estar publicado solicita su publicación.

Conclusiones: El proceso define 2 riesgos de corrupción, uno asociado a generación de condiciones normativas y otro a expedición de conceptos. Para este último riesgo, se definen las mismas causas del primer riesgo, así como 2 controles registrados en este. Dado lo anterior, se sugiere analizar la posibilidad de unificarlos en un solo riesgo de corrupción más robusto y que dé cuenta de la gestión del proceso.

Adicionalmente, se recomienda el fortalecimiento de los controles, atendiendo a que en la vigencia 2017 se identificó por parte de la Oficina de Control Interno, la materialización de un riesgo de corrupción en el proceso, generando la situación de mejora 1752 *"Se evidenció la materialización del riesgo de corrupción identificado por el proceso, Expedición de conceptos relacionados con la planeación territorial que favorezcan de manera indebida el interés de particulares, lo que en criterio de la OCI obedeció a que los controles tienen debilidades en su diseño; los criterios que definen su efectividad muestran que pese a que la actividad se adelanta, no previene ni mitiga el riesgo y resultan ineficaces; las clasificación de éstos no permite que el riesgo sea llevado a la zona de exposición extrema y darle el tratamiento adecuado; no atacan la causas detectadas; dentro de las causas no se identificó una relacionada con el sentido de pertenencia, los valores éticos o el empoderamiento individual de la gestión por parte de los funcionarios que intervienen en la elaboración de los productos y la prestación de los servicios y se cuenta con controles de tipo manual y no automáticos que permitan la utilización de herramientas tecnológicas como sistemas de información o software, diseñados para prevenir, detectar o corregir errores o deficiencias, sin que tenga que intervenir una persona en el proceso."*

Llama la atención, que aunque este proceso es de tipo misional y gestiona trámites tales como *Declaración de áreas de reserva para infraestructura y equipamientos de servicios públicos domiciliarios y las tecnologías de la información y de las comunicaciones – TICS, Consulta preliminar para la formulación de planes de implantación, Formulación del proyecto de plan de implantación,* entre otros, se evidenció que no se identificaron riesgos de corrupción asociados a éstos, atendiendo a que en su definición propiamente dicha tiene implícita la relación con terceros, que puede implicar posibles hechos de corrupción.

Lo anterior, en concordancia con lo establecido en el *Protocolo para la identificación de riesgos corrupción asociados a la prestación de trámites y servicios* del Departamento Administrativo de la Función Pública, que entre otras cosas indica que *"El resultado de la identificación de riesgos de corrupción se debe constituir en un criterio para la priorización de los trámites a intervenir mediante estrategias de racionalización, bien sea mediante acciones normativas, administrativas o tecnológicas de racionalización."*

4.3.13 PROCESO PRODUCCIÓN, ANÁLISIS Y DIVULGACIÓN DE LA INFORMACIÓN M-CA-003

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	SUBSECRETARÍA DE INFORMACIÓN
Proceso Nuevo	A-CA-009 GESTIÓN DEL SERVICIO A LA CIUDADANÍA E-CA-006 INTELIGENCIA PARA LA PLANEACIÓN E-CA-006 INTELIGENCIA PARA LA PLANEACIÓN

Objetivo del Proceso	Capturar, recolectar, administrar, actualizar, analizar y producir información estratégica del Distrito Capital y la región, mediante la gestión de información gráfica y alfanumérica y de las herramientas de focalización del gasto, la base de datos geográfica y los estudios socioeconómicos, con el fin de realizar el suministro de información para la toma de decisiones de la ciudadanía, administración distrital y partes interesadas, a través de los diferentes canales de atención.

Tipo de Riesgo	**Gestión**
Riesgos	Posibilidad de afectación económica y reputacional por deficiencia en la recolección, digitación y cargue de la información.
Causas	Diseños metodológicos internos y externos inapropiados y/o desactualizados, recursos insuficientes tanto para la actualización de tecnologías como para la capacitación en la recolección de información y deficiencia en la apropiación y aplicación de los instructivos o protocolos frente a la información recibida.
Riesgos	Posibilidad de afectación reputacional por reclamaciones o quejas de las partes interesadas, que podrían implicar actuaciones judiciales y disciplinarias.
Causas	Debido a la inexactitud en la entrega y divulgación de la información gráfica y alfanumérica a través de los diferentes canales de atención.

Conclusiones: Se sugiere revisar la identificación de nuevos riesgos, causas y controles o fortalecer los ya existentes, contemplando los hallazgos realizados en los informes de auditoria tanto Externas (Informe Definitivo de la Auditoría Interna del Sistema de Gestión de Calidad 2023, Informe de seguimiento consolidado sobre la calidad de las respuestas emitidas en el sistema distrital para la gestión de peticiones ciudadanas - Bogotá te escucha, correspondiente al mes de enero de 2023, secretaría general, dirección distrital de calidad del servicio) como internas (Informe Definitivo de Auditoría Interna al Proceso de Producción, Análisis y Divulgación de la Información M-CA-003) a su vez informe de la Contraloría de Bogotá en la Auditoría de Desempeño Sistema Bogotá Solidaria Código de Auditoría No. 215 Octubre de 2022.

Por otra parte, tener en cuenta las observaciones realizadas en el Informe monitoreo de segunda línea de defensa a los mapas de riesgos de gestión, corrupción y de seguridad de la información de la secretaría distrital de planeación con corte a 30 de abril de 2024, donde se evidenció que no estaba mencionado el trámite de Certificación de Estratificación Socioeconómica, el cual sigue vigente en el inventario de trámites y OPA en la entidad.

Tipo de Riesgo	**Corrupción**
Riesgos	Posibilidad de adulteración y /o manipulación por acción u omisión de la información oficial para beneficio privado.
Causas	1. Debilidad en la aplicación de los controles establecidos para la recolección, procesamiento y análisis y divulgación de la información. 3. Suministro de conceptos o de información errónea o inconsistente. 4. Manipulación indebida de recursos tecnológicos e información propia del proceso. 5. Desconocimiento por parte de la ciudadanía y usuarios sobre los productos y servicios relacionados con la información gráfica y alfanumérica que produce la entidad. 6. Incumplimiento del manual de funciones, procedimientos, código ético y políticas de seguridad de la información por parte de algunos servidores. 7. Manipulación indebida de la información recolectada para beneficio propio o de terceros (cuando es recolectada por entidades externas).

Conclusiones: Se sugiere la actualización o identificación de nuevos riesgos causas y controles conforme a los hallazgos realizados en Informe Definitivo de Seguimiento a la Atención de Peticiones, Quejas, Reclamos, Sugerencias, Atención a la Ciudadanía y Denuncias por Posibles Actos de Corrupción para el Segundo Semestre de 2022 y primer semestre del año 2023, tener en cuenta las observaciones realizadas en el Informe monitoreo de segunda línea de defensa a los mapas de riesgos de gestión, corrupción y de seguridad de la información de la secretaría distrital de planeación con corte a 30 de abril de 2024, donde se evidenció que no estaba mencionado el trámite de Certificación de Estratificación Socioeconómica, el cual sigue vigente en el inventario de trámites y OPA en la entidad.

Por otra parte, se recomienda en la descripción del riesgo redactar a qué clase de información oficial hace referencia y verificar que los controles ya identificados tengan relación directa con las seis (6) causas o fallas que puedan dar origen a la materialización del riesgo y que permitan mitigar dicho riesgo, por consiguiente, se sugiere que para cada causa se debe establecer o identificar un control o controles. Igualmente, puntualizar a que hace referencia los servidores de la dirección de registros sociales y cuál es el rol que ejerce en la ejecución del control, es importante establecer el cargo (profesional, técnico, coordinador o jefe). A su vez, los controles identificados no se registra la evidencia de la ejecución del control y donde quedan almacenados.

Finalmente, el plan de acción para el tratamiento del riesgo de 2024 registra la actividad de 3 jornadas de socialización de los procedimientos del proceso realizadas por cada una de las Direcciones de la Subsecretaría, pero no especifica a cuáles procedimientos se realizará, o si es a los 23 procedimientos registrados en el contexto de identificación de riesgos y no presenta la fecha de seguimiento de dicho plan de acción.

Tipo de Riesgo	**Seguridad de la Información**
Tipo de Activo	Software Información "SISBÉN" (Oracle) Aplicativo de registro de solicitud, de procesamiento y de consulta de encuesta Sisbén
Riesgo 1.	Posibilidad de pérdida de confidencialidad de la "Información Sisbén" registrada en Oracle por accesos abusivos al sistema informático si no hay mecanismos de identificación y autenticación adecuados que eviten el acceso de personas no autorizadas en el sistema que consulten usen o sustraigan la información de las encuestas; igualmente, se puede presentar una pérdida de la confidencialidad si la información de Oracle es hurtada.
Causa	Debido a fallas en la configuración correcta de los parámetros de seguridad del sistema contra software maliciosos o descargas ilegales de la base de datos por ejemplo
Objetivo de Control 1.	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
Control	El Líder administrador de la herramienta software debe verificar que los mecanismos de identificación y autenticación en el sistema funcionen adecuadamente, estableciendo restricciones a los posibles usuarios del sistema
Objetivo de Control 2.	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
Control	El líder administrador de la herramienta de software debe configurar los parámetros de seguridad del sistema y el servicio que Oracle presta internamente
Riesgo 2.	Posibilidad de pérdida de la disponibilidad de la información en el Aplicativo de Consulta Sisbén

Tipo de Riesgo	Seguridad de la Información
Causa	saturación del sistema imprevista al ser un software inmaduro, igualmente, se puede presentar un mal funcionamiento del software por fallas en el mismo al no hacer pruebas suficientes de software o que la información sea destruida y se pierda por no generar copias de respaldo suficientes y oportunas
Objetivo de Control 1.	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
Control	El líder funcional del aplicativo configura los lineamientos de prueba a aplicar previo a la implementación del sistema
Objetivo de Control 2.	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la información
Control	El líder funcional del aplicativo configura los lineamientos de prueba validando que las nuevas operaciones del sistema no generen riesgos de seguridad que afecten la disponibilidad de la información
Objetivo de Control 3.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control	El líder administrador de la Dirección de Tecnologías y las Comunicaciones establece acorde a las políticas de seguridad de la entidad y la criticidad de la información alojada en el aplicativo, la realización de las copias de respaldo
Riesgo 3.	Posibilidad de pérdida de integridad de la información por la denegación de servicios informáticos por parte del Departamento Nacional de Planeación -DNP
Causa	si los equipos donde se instala el aplicativo no se configuran correctamente de acuerdo a los parámetros técnicos y de seguridad requeridos. Igualmente, se pueden presentar perdidas en la integridad de la información por no hacer el mantenimiento adecuado del sistema conforme a las versiones de actualización que establezca el DNP.
Objetivo de Control 1.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
Control	El líder funcional del aplicativo en la Dirección debe coordinar con el área de Tecnologías de la Información y las Comunicaciones que se cumplan todas las condiciones de software y hardware para la instalación, ejecución y acceso al aplicativo según los parámetros del desarrollador, armonizando las condiciones técnicas a las políticas de seguridad de la información y de licencia de software
Objetivo de Control 2.	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.
Control	El líder funcional del aplicativo en la entidad verifica periódicamente que se la versión en uso del software corresponda a la actualizada
Riesgo 4.	Posibilidad de pérdida de confidencialidad de la información registrada en el aplicativo por copias fraudulentas que se hagan a las bases de datos que alimentan el sistema
Causa	Debido a una configuración incorrecta de los parámetros de seguridad que permitan éstas y otras acciones no autorizadas; igualmente es posible que se pierda la confidencialidad si terceros no autorizados logran falsificar sus derechos de acceso porque los controles de identificación y autenticación de usuarios no operan correctamente.
Objetivo de Control 1.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
Control	El Líder administrador de la herramienta software debe establecer los controles y restricciones necesarias para el acceso, descarga y copia de la información conforme a las políticas de seguridad de la entidad y la norma aplicable para el tratamiento de datos personales
Objetivo de Control 2.	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

Tipo de Riesgo	**Seguridad de la Información**
Control	El Líder administrador de la herramienta software configura los mecanismos de identificación y autenticación en el sistema para identificar a que usuarios se les autoriza el acceso a la información

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y se registran documentos como Actas Comité Técnico de SISBÉN, Actas Comisión Intersectorial de Estudios Económicos y de Información y Estadísticas del Distrito Capital entre otros y presentan niveles de criticidad Media, teniendo en cuenta la Confidencialidad, disponibilidad e integralidad de la información por lo que se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política de Administración del Riesgo y conforme a lo señalado en el numeral 4,7 Manejo de activos de la Política de gestión de activos A-LE-474, aplicando el modelo institucional de gestión de riesgos para identificar y tratar los riesgos que puedan afectar a los activos de información, que hagan parte del inventario de activos de información a su cargo y se encuentren clasificados en nivel de criticidad ALTA se debe gestionar dichos riesgos.

Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, no se detalla que pasa si el control falla. En la descripción del control se evidencian frecuencias anuales, periódicas y en otras no determina la periodicidad sin embargo en la matriz de riesgos, hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Finalmente, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación.

4.3.14 PROCESO SOPORTE LEGAL A-CA-003

Objetivo Estratégico	Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua.
Líder Proceso	SUBSECRETARÍA JURÍDICA
Proceso Nuevo	A-CA-013 GESTIÓN JURÍDICA
Objetivo del Proceso	Asesorar y representar jurídicamente a la SDP a través de la revisión y proyección de actos administrativos y conceptos y la representación judicial y extrajudicial.

Tipo de Riesgo	**Gestión**
Riesgos	Posibilidad de afectación económica y reputacional por incremento en fallos condenatorios en contra de la entidad y mala imagen institucional, debido a inadecuada apropiación de los temas, sistemas de información y términos para dar respuesta.
Causas	Incremento en fallos condenatorios en contra de la entidad y mala imagen institucional

Conclusiones: Se sugiere analizar la inclusión de nuevos riesgos causas y controles de acuerdo a los hallazgos identificados en el informe definitivo de evaluación y seguimiento a la gestión del comité de conciliación de la SDP y al Informe Definitivo de la Auditoría Interna del Sistema de

Gestión de Calidad 2023, a su vez contemplar riesgos por Posibilidad de dar respuestas imprecisas o mal fundamentadas que pueden afectar la toma de decisiones tanto del área como de la entidad, dar respuestas extemporáneas a consultas y peticiones. entre otras. Finalmente, en los controles identificados no se registra la evidencia de la ejecución del control y donde quedan almacenados

Tipo de Riesgo	**Corrupción**
Riesgos	Posibilidad de encausar y/o intervenir indebidamente en las actividades a cargo de la Subsecretaría Jurídica con el fin de obtener un pronunciamiento y/o una decisión administrativa con desviación de lo público y en beneficio propio o de un tercero
Causas	1. Presión de grupos sociales o de interés frente a temas de competencia de la SDP 2.Ofrecimiento o solicitud de dádivas en beneficio propio o de terceros

Conclusiones: Teniendo en cuenta el plan de acción para la vigencia 2024, con el fin de dar tratamiento al riesgo identificado y mitigar su nivel del riesgo se estableció realizar sensibilización a los servidores de la Subsecretaría Jurídica y sus dependencias, sobre implicaciones disciplinarias en el ejercicio de la función pública, se sugiere verificar dicha acción ya que no indica cual es la periodicidad con la que se realizaran las sensibilizaciones y cuantas se ejecutaran durante la vigencia,

Tipo de Riesgo	**Seguridad de la Información**
Tipo de Activo	Datos Información Proyección de conceptos, actos administrativos, documentos de acciones judiciales y conciliaciones extrajudiciales, que se proyecten o revisen en la Subsecretaría Jurídica de la SDP.
Riesgo.	Posibilidad de Pérdida de confidencialidad por fallas humanas, divulgación ilegal de la información y/o uso no autorizado de equipos en la proyección de conceptos, actos administrativos, documentos de acciones judiciales y conciliaciones extrajudiciales.
Causa	Debido a manejo manual de la información, desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, y/o información sensible sin cifrado
Objetivo de Control 1.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
Control	El Líder de proceso define la clasificación de la información que produce por medio del formato de registro de activos de información e índice de información clasificada y reservada.
Objetivo de Control 2.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	El Líder de Seguridad de la Información socializa las políticas de Sistema de Gestión de Seguridad de la Información y los lineamientos para el manejo adecuado de la información.
Objetivo de Control 3.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	El Líder de Seguridad de la Información genera las políticas de Sistema de Gestión de Seguridad de la Información y determina los lineamientos para el manejo adecuado de la información.

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y presenta niveles de criticidad Baja y Media, por lo que se sugiere evaluar la criticidad de estos activos con el fin de determinar si corresponde o están identificados con un nivel ALTO que según E-LE-030 Política De Administración del Riesgo se debe gestionar dichos riesgos. Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, no se detalla que pasa si el control falla. En la descripción del control se evidencian frecuencias anuales, periódicas y en otras no determina la periodicidad sin embargo en la matriz de riesgos, hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Finalmente, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación.

4.3.15 PROCESO SOPORTE TECNOLÓGICO A-CA-007

Objetivo Estratégico	Impulsar una estrategia de transformación digital de la SDP, por medio del desarrollo tecnológico de herramientas que permitan generar valor a los procesos misionales y los servicios digitales de la entidad para los grupos de valor e interés.
Líder Proceso	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Proceso Nuevo	E-CA-007 GOBIERNO DE TI
Objetivo del Proceso	Fortalecer, administrar y soportar los servicios de las tecnologías de la información y las comunicaciones TIC mediante la gestión integral de su operación, mantenimiento y actualización para impulsar la estrategia de transformación digital que permita generar valor a los procesos misionales y los servicios digitales de la entidad para los grupos de valor e interés de la Secretaría Distrital de Planeación.

Tipo de Riesgo	**Gestión**
Riesgo	Posibilidad de afectación reputacional por insuficiente destinación para cubrir las necesidades de la sostenibilidad y mejoramiento de la operación de servicios tecnológicos,
Causas	La variación de la Tasa Representativa del Mercado (TRM) y limitada asignación de recursos presupuestales.
Riesgo	Posibilidad de afectación reputacional por recurso humano insuficiente para soportar los diferentes servicios de tecnologías de la información con componente de infraestructura,
Causas	Aumento en la demanda de requerimientos y crecimiento en componentes de infraestructura tecnológica de la Entidad.
Riesgo	Posibilidad de afectación reputacional por cambios en los requerimientos funcionales pactados en el instrumento a-fo-227 al momento de la entrega de la solución de software al usuario funcional,
Causas	Insuficiente dimensionamiento del alcance y de los requerimientos entre el nivel Directivo y el usuario funciona
Riesgo	Posibilidad de afectación reputacional por insuficiente alineación de las áreas externas a tecnología frente a los procedimientos, estándares y herramientas establecidos por la dirección de tic para la construcción y mantenimiento de soluciones de software,
Causas	Desarticulación entre los procesos de la entidad con el proceso de Gobierno de TI, Incumplimiento de las políticas y procedimientos establecidos para el desarrollo y mantenimiento del software

Tipo de Riesgo	Gestión
Riesgo	Posibilidad de afectación reputacional por reprocesos por la falta de continuidad en la prestación del servicio por parte del contratista de mesa de ayuda con personal idóneo y capacitado,
Causas	Pérdida de conocimiento por la rotación y poca trazabilidad del conocimiento específico de los roles
Riesgo	Posibilidad de afectación reputacional por falta de oferta de servicios de soporte y garantías para componentes de ti,
Causas	Obsolescencia tecnológica
Control 1	El (la) profesional que ejerce el rol de líder del equipo de soporte con base en el informe de laboratorio cada vez que se requiera, valida las razones para tomar la decisión de reparar los elementos tecnológicos o dar concepto para baja en el inventario a través de la expedición del concepto técnico en el documento correspondiente e informa a las dependencias pertinentes para adelantar las acciones a que haya lugar. Si existen inconsistencias se verifica en la herramienta de mesa de ayuda si el documento se aportó como evidencia y se encuentra debidamente diligenciado.
Control 2	El (la) profesional que ejerce el rol de líder del equipo de soporte cada vez que se requiere coteja el estudio de mercado de las partes/repuestos con fines de aprobar la adquisición de las mismas por parte del contratista de la mesa de ayuda a través del concepto técnico en el documento correspondiente e informa a las dependencias pertinentes para adelantar las acciones a que haya lugar. Si existen inconsistencias se reprocesa la fase inicial de estudios de mercado.

Conclusiones: Se sugiere revisar la identificación de nuevos riesgos, causas y controles o fortalecer los ya existentes, contemplando los hallazgos realizados en los informes de auditoria internos como el Informe de Seguimiento al Modelo de Seguridad y Privacidad de la Información para la vigencia 2023 con Posibles efectos de Riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP por no contar con recursos para la adquisición e implementación de herramientas de software para la realización de copias de seguridad de la información institucional, así como tampoco para la actualización del licenciamiento de la solución del antivirus, disminución de recursos significativos para realizar las actividades de la «FASE I para la Migración de servicios tecnológicos de la entidad a la nube» y la «Operacionalización del Plan de Recuperación de Desastres.», entre otros. Así como los hallazgos realizados en el Seguimiento de la gestión a las Mesas de Apoyo/Ayuda lideradas por la Dirección Administrativa y por la Dirección de Tecnologías de la Información y las Comunicaciones y al Informe Definitivo de la Auditoría Interna del Sistema de Gestión de Calidad 2023. Se recomienda la revisión de los controles 1 y 2 del sexto riesgo identificado, ya que fueron catalogados como correctivos, sin que se relacionara con la gestión en el evento de una materialización de riesgos.

Tipo de Riesgo	Corrupción
Riesgos	Posibilidad de asignación indebida de permisos para el acceso y uso de servicios tecnológicos no autorizados con el fin de obtener beneficio propio o de un tercero
Causas	1. Omitir intencionalmente los procedimientos y políticas para el control de acceso y uso de servicios tecnológicos. 2. Ausencia de controles automatizados en las soluciones de software que pueden facilitar el acceso a la información y su posible manipulación o adulteración.

Conclusiones: Se sugiere verificar y analizar la periodicidad con la que se ejecuta el segundo control, e cual se realiza anualmente por periódicamente teniendo en cuenta el flujo o movimiento

de funcionarios y contratistas dentro de la entidad con el fin de minimizar los accesos a la información, y fortalecer el plan de acción para el tratamiento del riesgo que es la Implementación de doble factor de autenticación para el ingreso a los sistemas de información y/o aplicaciones priorizadas.

Tipo de Riesgo	**Seguridad de la Información**
Tipo de Activo	Hardware (1) Soluciones de Procesamiento (2) Soluciones de Conectividad (3) Equipos de Seguridad (4) Solución de Almacenamiento (5) Infraestructura Puestos de Trabajo (6) Solución de Backup y (7) UPS Software (1) Soluciones de software Misional (2) Direccionamiento Estratégico (3) Procesos de Apoyo (4) Procesos de Evaluación del A-LE-445 Catálogo de Sistemas de Información de la SDP (Anexo 3 PETI) datos Información Información producida por el proceso de gestión tecnológica**.**
Riesgo 1.	Posibilidad de Pérdida de Disponibilidad de los activos de información tipo hardware por fallas y/o mal funcionamiento del equipo, fallas generadas por inadecuadas condiciones físicas y ambientales y hurto de información y/o equipo de cómputo que hacen parte de la infraestructura tecnológica de la Entidad,
Causa	Debido a insuficiente mantenimiento (físico, lógico y aseguramiento), obsolescencia tecnológica tipo hardware, susceptibilidad a las variaciones físicas (humedad, polvo, suciedad, voltaje, temperatura, sensibilidad electromagnética) y acceso al hardware sin protección o protocolos de seguridad.
Objetivo de Control 1.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
Control	El (la) profesional que ejerce el rol de líder del equipo de soporte e infraestructura de la Dirección de TIC, anualmente actualizan el "Plan de mantenimiento de infraestructura tecnológica de la SDP" y verifican de forma aleatoria el mantenimiento preventivo programado, registrando la información en el formato de reunión A-FO-184 referente al plan de mantenimiento. En caso de que existan situaciones atípicas o fuera de este plan, el profesional que ejerce el rol de líder del equipo de infraestructura convocará a reunión con quien corresponda y se dejará acta de reunión y compromisos. En caso de inconsistencias se informa al Director de TIC y se realizan los ajustes que se determinen.
	El (la) profesional que ejerce el rol de líder del equipo de soporte e infraestructura de la Dirección de TIC cada vez que se requiera, actualizan el "Plan de mantenimiento de infraestructura tecnológica de la SDP" y verifican de forma aleatoria el mantenimiento correctivo (bolsa de repuestos por cambio de partes) programado, registrando la información en el formato de reunión A-FO-184 referente al plan de mantenimiento. En caso de que existan situaciones atípicas o fuera de este plan, el líder convocará a reunión con quien corresponda y se dejará acta de reunión y compromisos. En caso de inconsistencias se informa al Director de TIC y se realizan los ajustes que se determinen.
Objetivo de Control 2.	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
Control	El (la) profesional que ejerce el rol de operador (a) del centro de cómputo, diariamente ejecuta la verificación de los equipos activos de red, aire acondicionado, fibras de

Tipo de Riesgo	Seguridad de la Información
	conexión, UPS, servidores, switch, revisión de URLs de aplicaciones como se describe en el procedimiento sobre "Monitoreo de la Infraestructura Tecnológica de la SDP" ingresando para ello en cada uno de los Centros de cableado y Data center con el objetivo de revisar el funcionamiento de cada elemento y en caso de encontrarse inconvenientes se registra una nueva solicitud en la herramienta de mesa de ayuda escalando a segundo nivel y dejando evidencia de ello en la bitácora de monitoreo. En caso de encontrar inconsistencias o fallas en los equipos se informa al Director (a) para establecer las acciones correspondientes.
	El (la) profesional que ejerce el rol de operador (a) del centro de cómputo, diariamente revisa el estado de los servidores de procesamiento y almacenamiento a través de herramientas de monitoreo disponibles. En caso de encontrar inconsistencias informa al Director (a) mediante correo electrónico para tomar las acciones respectivas.
Objetivo de Control 3.	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Control	Los (las) profesionales del equipo infraestructura y de soporte cada vez que se requiera generarán controles de cambio informático, para realizar acciones sobre la infraestructura tecnológica que mitigue el riesgo de indisponibilidad, dejando evidencia de las actividades en el plan de seguimiento de cada control de cambio. En caso de presentarse novedades se informa al Director (a) para los realizar los ajustes correspondientes.
Objetivo de Control 4.	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
Control	El (la) profesional que ejerce el rol de líder del equipo de infraestructura y demás profesionales anualmente formulan y ejecutan el plan de acción para la gestión de vulnerabilidades, las cuales se identifican por medio de la herramienta de escaneo de la Entidad. En el evento de encontrar inconsistencias se informan al Director (a) para gestionar las acciones necesarias.
Riesgo 2.	Posibilidad de Pérdida de Integridad de los activos de información tipo hardware que hacen parte de la infraestructura tecnológica de la Entidad por uso no autorizado del equipo,
Causa	Debido al acceso sin protección o protocolos de seguridad.
Objetivo de Control 1.	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
Control	El (la) profesional que ejerce el rol de Oficial de Seguridad de la Información de la Entidad anualmente gestiona la depuración de usuarios activos e inactivos con acceso privilegiado a los activos de información tipo hardware, de acuerdo a los eventos evidenciados por parte del equipo auditor en la revisión de los controles del Sistema de Gestión de la Seguridad de la Información. En caso de presentar novedades se informa al Director (a) para establecer las medidas respectivas.
Objetivo de Control 2.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
Control	El (la) profesional que ejerce el rol de Oficial de Seguridad de la información, cada vez que se requiera, apoya el seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información y gestiona las situaciones susceptibles de mejora encontradas. En caso de presentar novedades se informa al Director (a) de TIC y se toman las acciones correspondientes.
Objetivo de Control 3.	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

Tipo de Riesgo	**Seguridad de la Información**
Control	El (la) supervisor (a) o a quien este (a) delegue, cada vez que se requiera, realiza acompañamiento y monitoreo a las actividades de los proveedores de servicios (mantenimiento, vigilancia, implementaciones, obras civiles) en las áreas seguras como el Datacenter (actividades programadas por la DTIC), Centros de cableado y Centro de cómputo. En caso de inconsistencias el (la) delegado, informa al Director (a) de TIC para tomar las medidas necesarias.
Objetivo de Control 4.	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
Control	El (la) profesional que ejerce el rol de Oficial de Seguridad de la Información de la Entidad anualmente, realiza seguimiento al cumplimiento de la Política de Seguridad Física y del Entorno y ejerce inspección a los controles de acceso físico (puertas, sistema biométrico, llaves). En caso de encontrar novedades informa al Director (a) de TIC para realizar las acciones respectivas.
Objetivo de Control 5.	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
Control	El (la) profesional que ejerce el rol de Oficial de Seguridad de la Información y la Dirección Administrativa anualmente, verifica cada vez que se requiera, la aplicación de los controles establecidos en el documento A-LE-452 Política de Seguridad Física y del Entorno relacionadas con el acceso a las áreas seguras. En el evento de encontrar novedades se informa al Director (a) de TIC para realizar las acciones respectivas.
Riesgo 3.	Posibilidad de Pérdida de Disponibilidad en los activos de información tipo software relacionados en el Catálogo de sistemas de información por fallas humanas, destrucción o pérdida de la información, error en el uso o abuso de derechos y privilegios, acceso abusivo a sistema informático, mal funcionamiento de software y explotación de brechas de seguridad en las diferentes capas que soportan la solución de software
Causa	Debido a configuración incorrecta de parámetros, ausencia de copias de respaldo de los sistemas de información, insuficiente aplicación de las políticas de seguridad y privacidad de la información, habilitación de servicios innecesarios, ausencia o insuficiencia de pruebas de software y obsolescencia tecnológica.
Objetivo de Control 1.	Se debe restringir el acceso a los códigos fuente de los programas.
Control	El (la) profesional que ejerce el rol de líder del equipo de software cada vez que se requiera, solicita para que, a través del repositorio dispuesto por la Dirección de TIC, se asignen los roles para el acceso al equipo de desarrolladores. En caso de inconsistencias el (la) delegado, informa al Director (a) de TIC para tomar las medidas necesarias.
Objetivo de Control 2.	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
Control	El (la) profesional que ejerce el rol de líder del equipo de software cada vez que se requiera, prepara y convoca reunión al equipo de gestión del cambio de la Dirección de TIC para presentar el control de cambio informático para el despliegue en ambiente de producción, sujeto de aprobación. En caso de inconsistencias se informa al Director (a) de TIC para tomar las medidas necesarias.
Objetivo de Control 3.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
Control	El (la) profesional que ejerce el rol de líder del equipo de software cada vez que se requiera, solicita a través de solicitud en la mesa de ayuda la inclusión o realización de la copia de respaldo de la solución de software en el plan de backup. En el evento de encontrar novedades se informa al Director (a) de TIC para realizar las acciones respectivas.

Tipo de Riesgo	**Seguridad de la Información**
Objetivo de Control 4.	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
Control	El (la) profesional que ejerce el rol de líder del equipo de software cada vez que se requiera, solicita al Director de TIC el registro de la solicitud en la mesa de ayuda para la realización del análisis del vulnerabiliades sobre el software propietario, solicitud que va dirigida al o (a la) líder del equipo que gestiona la herramienta de escaneo de vulnerabilidades. En caso de encontrar novedades informa al Director (a) de TIC para realizar las acciones respectivas.
Objetivo de Control 5.	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
Control	El (la) profesional de desarrollo del equipo de software cada vez que requiera, verifica junto con el usuario funcional el formato A-FO-225 para realizar pruebas funcionales y no funcionales durante la fase de pruebas, previo a la fase de puesta en operación. En caso de presentar novedades se informa al Director (a) de TIC y se toman las acciones correspondientes.
Objetivo de Control 6.	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.
Control	El (la) profesional que ejerce el rol de Oficial de seguridad de la información cada vez que se requiere, ejecuta las revisiones sobre el cumplimiento de las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información. En el evento de encontrar novedades se informa al Director (a) de TIC para realizar las acciones respectivas.
Riesgo 4.	Posibilidad de Pérdida de Confidencialidad en los activos de información tipo software relacionados en el Catálogo de sistemas de información por fallas humanas, falsificación de derechos de acceso y divulgación ilegal de la información
Causa	Debido a configuración incorrecta de parámetros, gestión deficiente de la contraseñas - contraseñas sin protección y asignación errada de los derechos de acceso.
Objetivo de Control 1.	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
Control	El (la) profesional que ejerce el rol de líder del equipo de software anualmente define las aplicaciones críticas para que desde el equipo de infraestructura se realice el aseguramiento con la implementación del certificado seguro en los servidores de aplicación. En caso de presentar novedades se informa al Director (a) de TIC y se toman las acciones correspondientes.
Objetivo de Control 2.	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
Control	El (la) profesional que ejerce el rol de líder del equipo de software junto con el equipo de desarrollo cada vez que se requiere, realiza la actualización del versionamiento del software base y migración de soluciones de software a infraestructura asegurada. En caso de presentar novedades se informa al Director (a) para establecer las medidas respectivas.
Objetivo de Control 3.	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
Control	El (la) profesional que ejerce el rol de líder del equipo de software y/o el profesional de desarrollo cada vez que se requiere, solicita al usuario funcional (como área responsable del dato) el registro del requerimiento con fines de entrega o restauración de datos de pruebas. En caso de inconsistencias se informa al Director de TIC y se realizan los ajustes que se determinen.

Tipo de Riesgo	Seguridad de la Información
Objetivo de Control 4.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
Control	El (la) profesional que ejerce el rol de oficial de seguridad anualmente realiza la depuración de usuarios en cumplimiento del Procedimiento A-PD-104 Gestión Cuentas de Usuario. En caso de inconsistencias se informa al Director (a) de TIC para tomar las medidas necesarias.
Riesgo 5.	Posibilidad de Pérdida de Confidencialidad por divulgación ilegal de la información, ingeniería social, y uso no autorizado del equipo; relacionada con la información producida por el proceso de gestión tecnológica,
Causa	Debido al desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, ausencia de validación de autenticación de la información sensible sin cifrado
Objetivo de Control 1.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
Control	El (la) profesional que ejerce el rol de oficial de seguridad anualmente revisa con fines de actualización y cada vez que se requiera define nuevas políticas de seguridad y privacidad de la información. Estas políticas pueden ser consultadas a través herramientas dispuestas por la Entidad y en los espacios de capacitación y sensibilización vigente. En el evento de encontrar novedades se informa al Director (a) de TIC para realizar las acciones respectivas.
Objetivo de Control 2.	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
Control	El (la) profesional que ejerce como líder del equipo de infraestructura permanentemente, asegura la aplicación de la política del directorio activo de bloqueo de pantalla de los equipos de los funcionarios después de un tiempo determinado de inactividad. En el evento de encontrar novedades se informa al Director (a) de TIC para realizar las acciones respectivas.
Objetivo de Control 3.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
Control	El (la) profesional que ejerce el rol de oficial de seguridad, cada vez que se requiera, lidera el proceso de actualización de los registros de activos de información e índice de información clasificada y reservada de la entidad. En caso de inconsistencias se informa al Director (a) de TIC para tomar las medidas necesarias.

Conclusiones: Se verificó el A-LE-283 Registro de Activos de Información (RAI) y se registran 16 Activos de información con un nivel de clasificación o criticidad ALTA por tipología por ejemplo para Hardware Servidores Blade Producción Sin Alta Disponibilidad, Servidores Rack producción, Appliance Firewall, Solución de Backup, Equipos Routers, EXINDA 8064, Solución de Hiperconvergencia, Solución de Almacenamiento, Switch de Almacenamiento, para Software como Subversión, Software Comercial Data protector, Software Estratificación Urbana como herramientas para el manejo de estos activos los cuales no se evidencian en los riesgos identificados, por lo anterior se recomienda verificar y actualizar estos tipos de activos de información conforme a lo señalado en el numeral 4.7 *Manejo de activos de la Política de gestión de activos A-LE-474 "aplicando el modelo institucional de gestión de riesgos para identificar y tratar los riesgos que puedan afectar a los activos de información, que hagan parte del inventario de activos de información a su cargo y se encuentren clasificados en nivel de criticidad ALTA".* Lo anterior, alineado con Guía para la administración del riesgo y el diseño de controles en entidades públicas de DAFP, Guía 5 - *"Guía para la Gestión y Clasificación de Activos de información: seguridad y privacidad de la información"* del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia y los documentos del Sistema de Gestión de la Entidad: A-LE-505 Plan de tratamiento de Riesgos de Seguridad y Privacidad

de la Información. Es importante, atender lo indicado en el *Informe de Auditoría de Sistemas de Gestión* de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

Por otra parte, se recomienda verificar y ajustar los controles ya que en algunos casos no hay relación entre el objetivo control y la actividad de control, se entienden como dos actividades diferentes, es necesario que la una sea consecuencia de la otra ya que el control da el detalle de ejecución y el objetivo define el para qué se realiza el control. Así mismo, no se detalla que pasa si el control falla. En la descripción del control se evidencian frecuencias anuales, periódicas y en otras no determina la periodicidad sin embargo en la matriz de riesgos, hace referencia a una frecuencia con la que se realiza la actividad como diaria se sugiere unificar los criterios de evaluación. Finalmente, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación.

4.3.16 Riesgos del Sistema de Seguridad y Salud en el Trabajo

Dentro del presente seguimiento, se incluye este aparte donde se analizaron elementos del Sistema de Seguridad en el Trabajo, relacionados con la gestión de riesgos efectuada, con énfasis en la *Matriz de Identificación de Peligros, Evaluación y Valoración de los Riesgos* (A-LE-024), Versión 7 de diciembre de 2023.

De acuerdo con la matriz, se presentan 5 Grupos de Exposición Similar – GES (Conjunto de trabajadores que comparten un mismo perfil de exposición hacia un agente o conjunto de agentes) con la siguiente descripción:

Tabla N. 16. Clasificación por Grupos de Exposición Similar GES N.

Nº GES	DESCRIPCIÓN	CARGOS	Nº PERSONAS
GES Nº 1	Personal Administrativo	Secretario(a) Distrital, Subsecretario(a), Director(a), Técnico(a), Jefes de Oficina Asesora, Asesor, Jefes de Oficina, Profesional Universitario, Profesional Especializado, Técnicos Operativos, Auxiliar Administrativo, secretaria ejecutiva, contratista	1143
GES Nº 2	Personal Mantenimiento Dirección Administrativa.	Técnico Operativo, contratista	3
GES Nº 3	Personal Archivo Central Especializado, Biblioteca y Planoteca Dirección Administrativa	Profesional Universitario, Profesional Especializado, Técnicos Operativos, Auxiliar Administrativo	25
GES Nº 4	Conductores Dirección Administrativa	Conductor Mecánico.	16
GES Nº 5	Contratistas Aseo y Cafetería - Vigilancia y Seguridad Privada - - Dirección Administrativa	Auxiliar de Aseo y Cafetería. Guarda de seguridad	47

Fuente: A-LE-024 Matriz de Identificación de Peligros, Evaluación y Valoración de Riesgos -SDP Versión 7

Se evidenció que en la definición de los grupos 1 y 2 se incluyen contratistas, aunque en las matrices se registran actividades a cargo de contratistas en los grupos 2, 3 y 5, por lo que se sugiere la revisión de la información registrada. La matriz contiene 6 tipos de peligros en los que confluyen 218 situaciones contenidas en los GES definidos como se muestra a continuación:

Tabla N. 17. Tipología de riesgos de SST por cada Grupos de Exposición Similar - GES

Clasificación / Riesgo	GES 1	GES 2	GES 3	GES 4	GES 5	Total	%
Condiciones de Seguridad (Mecánico Mecanismos en movimiento, superficies calientes, proyección de partículas calientes. Uso de herramientas manuales; otros: Deportivos, Recreativos y Culturales Lesión en Actividad Física Deportiva o Recreativa; Público Robos, atracos, asaltos, atentados, de orden público; Tecnológico Incendio y explosión; Trabajo en Alturas Caídas; Colisiones, volcamientos; Eléctrico Baja tensión y electricidad estática.)	56	9	24	9	9	107	49,08%
Biomecánico (Esfuerzo Físico, visual, miembros superiores e inferiores, manipulación de cargas, movimiento repetitivo, postura prolongada mantenida (de pie, posición antigravitacional, incomodas).	21	5	14	3	7	50	22,94%
Psicosocial (Autonomía y reconocimiento; Identificación con la actividad; Comunicación, tecnología, organización del trabajo demanda cuantitativas de la labor, sistemas de control; Condiciones de la tarea - Monotonía, rutina en la labor; Demandas cualitativas y cuantitativas de la labor. Demandas de carga mental, emocionales; especificación de los sistemas de control; Esfuerzo fisiológico que demanda la ocupación, generalmente en términos de postura corporal, fuerza, movimiento y traslado de cargas e implica el uso de los componentes del sistema osteomuscular, cardiovascular y metabólico; Estrés, ansiedad, depresión; Gestión organizacional (evaluación del desempeño); Ritmo de trabajo, volumen de trabajo, funciones del cargo, responsabilidad; Sistemas de control para la seguridad de la tarea)	13	6	1	3	2	25	11,47%
Físico (Luz visible por exceso o deficiencia; Ruido (continuo, intermitente); Vibración)	5	2	4	2	1	14	6,42%
Químico (Gases y vapores; Líquidos (Contacto con sustancias); químicas por ejecución de protocolos de bioseguridad); Material particulado)	1	2	1	1	5	10	4,59%
Biológico (Bacterias, virus, hongos; Parásitos, Fluidos o excrementos)	3	1	3	1	4	12	5,50%
Total	**99**	**25**	**47**	**19**	**28**	**218**	
%	**45,41%**	**11,47%**	**21,56%**	**8,72%**	**12,84%**	**45,41%**	

Fuente: A-LE-024 Matriz de Identificación de Peligros, Evaluación y Valoración de Riesgos -SDP Versión 7

A continuación, se presenta la valoración de los riesgos de acuerdo con su clasificación, donde se observa que en su mayoría se encuentran en valoración media. Existen 3 situaciones valoradas *Muy Alto* relacionadas con *Lesiones, Politraumatismos, muerte* por *Accidentes de tránsito Colisiones, volcamientos;* y *Caída de objetos, tropezones, caídas, golpes* por *Locativo Condiciones de orden y aseo.*

Tabla N. 18. Valoración Riesgos

Valoración del Riesgo / Clasificación Riesgo	Muy alto	Alto	Medio	Bajo	Total	%
ACEPTABLE CON CONTROL ESPECIFICO (II)	**3**	**25**	**101**	**21**	**150**	**68,81%**
Biológico			8		8	3,67%
Biomecánico			38		38	17,43%
Condiciones de Seguridad	3	13	49	21	86	39,45%
Psicosocial		12	4		16	7,34%
Químico			2		2	0,92%
MEJORABLE(III)		**2**	**59**	**7**	**68**	**31,19%**
Biológico			4		4	1,83%
Biomecánico			11	1	12	5,50%
Condiciones de Seguridad		2	18	1	21	9,63%
Físico			11	3	14	6,42%
Psicosocial			8	1	9	4,13%
Químico			7	1	8	3,67%
Total	**3**	**27**	**160**	**28**	**218**	**100,00%**
%	**1,38%**	**12,39%**	**73,39%**	**12,84%**	**100,00%**	

Fuente: A-LE-024 Matriz de Identificación de Peligros, Evaluación y Valoración de Riesgos -SDP Versión 7

Se recomienda la evaluación de la valoración de las situaciones relacionadas con eventos deportivos, atendiendo que se presentaron varios accidentes de trabajo relacionadas con estas actividades. Es así como del reporte de incidentes, se solicitaron y revisaron soportes de los accidentes de trabajo ocurridos en la vigencia 2023 y lo corrido 2024. De los 10 ocurridos en 2023, se observa el diligenciamiento del Formato de investigación de incidentes, accidentes laborales y enfermedad de origen laboral SDP (A-FO-402), sin que se evidenciaran las firmas de los intervinientes por parte de seguridad y salud en el trabajo, accidentado, jefe inmediato y COPASST, siendo esto esencial para la autenticidad, formalización, oficialización y salvaguarda de los documentos como soportes de las investigaciones. Adicionalmente, en los campos *Jefe Inmediato* y COPASST no se presentan los nombres respectivos.

En cuanto al Plan Anual de Seguridad y Salud en el Trabajo, se verificó su publicación como anexo al Plan de Acción de la Entidad[1], el cual corresponde al documento A-LE-020 *Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST* Versión 12 de enero de 2024.

Por otra parte, de acuerdo con lo establecido en el artículo 2.2.4.6.11. y numeral 6 del artículo 2.2.4.6.12. del Decreto 1072 de 2015, se indagó sobre el programa de capacitación en seguridad y salud en el trabajo -SST vigencias 2023 y 2024, sin que se anexara el programa de 2023. Para esta vigencia, se adjuntó un reporte de Plan de Capacitación Anual 2024 que detalla Programa y Tema. Dado lo anterior, se recomienda fortalecer este plan para que se visibilicen variables como cantidad de capacitaciones programadas, fechas previstas, población objetivo, entre otros, que permitan realizar seguimiento del cumplimiento de las actividades propuestas a nivel de todas las líneas de defensa. Además, se sugiere que para la programación de este plan se tengan en cuenta los resultados de las mediciones realizadas sobre el sistema como insumo que propenda por la efectividad de las capacitaciones programadas.

Referente a su ejecución, se anexó reporte de 81 eventos ejecutados en el segundo semestre 2023, es decir, en promedio 14 eventos, con un ingreso promedio de 24 personas por evento, como se muestra en la siguiente tabla:

[1] https://docs.google.com/document/d/1BoQ86gaVNfr-2rLCvurYVs-9L9poTaBM/edit#heading=h.4k668n3

Tabla N. 19. Participación Eventos por Programa
Vigencia 2023

Programa	Eventos		Participantes	
	Cantidad	%	Cantidad	%
Medicina Preventiva	18	22,22%	747	38,70%
Prevención Desordenes Osteomusculares	28	34,57%	608	31,50%
Emergencias	11	13,58%	299	15,49%
Prevención Riesgo Psicosocial	10	12,35%	136	7,05%
Comité paritario de Seguridad y Salud en el Trabajo COPASST	6	7,41%	46	2,38%
Seguridad Vial	3	3,70%	43	2,23%
Estilos de vida y Hábitos Saludables	1	1,23%	29	1,50%
Comité de Convivencia Laboral CCL	3	3,70%	22	1,14%
Sala amiga de la Familia lactante	1	1,23%	0	0,00%
Total / promedios	**81**	**14**	**1.930**	**24**

Fuente: Reporte remitido "Evidencias capacitaciones y actividades 2023"

Nota: Se tomó el mayor valor de participantes al comparar las columnas número de participantes evidencia fotográfica y número de participantes registro de asistencia

Con corte a abril de 2024, se realizaron 52 eventos con una participación promedio de 33 participantes:

Tabla N. 20. Participación Eventos por Programa
Vigencia 2024

Programa	Eventos		Participantes	
	Cantidad	%	Cantidad	%
Comité Paritario de Seguridad y Salud en el Trabajo COPASST	2	3,85%	16	0,92%
Emergencias	3	5,77%	49	2,83%
Estilos de vida y hábitos saludables	25	48,08%	1096	63,21%
Prevención desordenes osteomusculares	20	38,46%	553	31,89%
Seguridad vial	2	3,85%	20	1,15%
Total / promedios	**52**	**13**	**1.734**	**33**

Fuente: Reporte remitido "Evidencias capacitaciones y actividades 2024"

Nota: Se tomó el mayor valor de participantes al comparar las columnas número de participantes evidencia fotográfica y número de participantes registro de asistencia

Dado lo anterior, la Oficina de Control Interno recomienda establecer mecanismos efectivos que incentiven la participación de los funcionarios y contratistas.

Complementario a lo anterior, en cumplimiento del artículo 2.2.4.6.21. del Decreto 1072 de 2015, se solicitaron los Indicadores que evalúan el proceso del Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST, se recibió y analizó el reporte de los 20 indicadores del sistema de seguridad y salud para la vigencia 2023, observando cumplimiento parcial en los siguientes 8 indicadores:

Tabla N. 21. Indicadores con cumplimiento inferior a 100

Nombre del indicador	Meta	Resultado alcanzado	Brecha	% Brecha
Evaluación Inicial SG SST	100	96	4	4,00%
Ejecución del Plan de Capacitación	80	0	80	100,00%
Evaluación de las Condiciones de Salud de los Colaboradores	100	90	10	10,00%
Evaluación de las Condiciones de Trabajo de los Colaboradores	100	90	10	10,00%
Cumplimiento en la Investigación de Incidentes, Accidentes y Enfermedades Laborales	100	0	100	100,00%
Frecuencia de Accidentes de Trabajo	10	0	10	100,00%
Severidad de Accidentes de Trabajo	20	0	20	100,00%
Ausentismo por Causas Relacionadas con la Salud	30	0,04	29,96	99,87%

Fuente: Reporte de Indicadores 2023

Llama la atención que 4 indicadores reflejan un resultado de cero, lo que se puede interpretar como la no realización de actividades para su cumplimiento. Sin embargo, al confrontar estos resultados con la ejecución del plan de trabajo del 2023, se detectan diferencias en los datos suministrados. Por ejemplo, la Ejecución del Plan de Capacitación se reporta un resultado de 0 en este reporte mientras que del plan de trabajo del 2023 se evidencian una serie de capacitaciones realizadas, reporta su cumplimiento al 100%. Situación similar se evidencia con el indicador *Cumplimiento en la Investigación de Incidentes, Accidentes y Enfermedades Laborales*. Dado lo anterior, la Oficina de Control Interno recomienda, por una parte, establecer mecanismos de control que permitan reflejar información coincidente en los diferentes instrumentos de reporte de información y se ajusten a la realidad de las actividades desarrolladas. Por otra parte, se sugiere para aquellos indicadores que no alcancen su cumplimiento, se considere la posibilidad de establecer planes de mejoramiento como una herramienta de mejora que permita registrar aquellas acciones de mejora establecidas en el proceso, así como el seguimiento a través de todas las líneas de defensa.

Por otra parte, se solicitó informe de la auditoría realizada en la vigencia 2023 al Sistema de Seguridad y Salud en el Trabajo (SSST), por lo cual la Dirección de Talento Humano remite documento *"Tabla de valores y calificación Estándares Mínimos SG-SST"* del 22 de diciembre de 2023, donde se registra una calificación total de 96 sobre 100, respecto de 60 preguntas de los estándares evaluados. El único incumplimiento registrado, corresponde al estándar *"Identificación de peligros, evaluación y valoración de los riesgos"*, donde en el numeral 4.1.4 "*Realización mediciones ambientales, químicas, físicas y biológicas"* se calificó en incumplimiento, dejando la siguiente recomendación: "*La empresa debe Realizar mediciones ambientales de acuerdo con los riesgos identificados en la matriz de riesgos y peligros, (Riesgos, Químico, Biológicos, Material particulado, Ruido, Iluminación, Temperatura y vibraciones), para esto debe contratar el servicio mediante una entidad o persona que cumpla con los requisitos para poder realizar este tipo de medición, se requiere un profesional en seguridad y salud en el trabajo, especialista en seguridad y Salud en el Trabajo o profesional en ingeniería con especialización en seguridad y salud en el trabajo, además de que cuenten con los equipos idóneos, debidamente certificados, ellos se encargarán de hacer la medición y de entregar un informe de resultados; a partir de allí la empresa deberá implementar las medidas necesarias para la intervención del riesgo. Adicional a esto la empresa debe Manejar un indicador para el tema del cumplimiento de mediciones ambientales el cual deberá medir anualmente."*

Complementariamente, a la pregunta relacionada con las mediciones ambientales ocupacionales y sus resultados de que trata el artículo 2.2.4.6.21. del Decreto 1072 de 2015, se indica que como plan de mejora ya se encuentran programadas para la vigencia del 2024, remitiendo correo electrónico con programación de visita para medición de iluminación.

Igualmente, en el cuestionario se indagó sobre la gestión realizada a las acciones desarrolladas resultado de las observaciones generadas en los mismos y si se han estructurado planes de mejoramiento para tratar las observaciones generadas, a lo que la Dirección de Talento Humano señaló que se realiza gestión con ARL para programar mediciones higiénicas como plan de mejoramiento.

Adicionalmente, en cumplimiento del artículo 2.2.4.6.21. del Decreto 1072 de 2015, el área remite el A-LE-021 *Plan de prevención, atención y respuesta a emergencias SDP Versión 6 de 2023*, el cual contiene el marco legal y técnico para preparación y respuesta a emergencias, generalidades de la entidad, descripción de los elementos estructurales, evaluación, plan operativo, atención primaria de las

emergencias, plan de contingencias y plan de emergencia seguridad vial. Igualmente, se anexa el *Informe de inspección técnica elementos para la atención de emergencias,* realizado por Positiva Compañía de Seguros en marzo de 2024, con 43 hallazgos como resultado de las inspecciones realizadas, indicando que *"con el objeto que puedan realizar medidas u oportunidades de mejora."*. A continuación, se enumeran las principales:

- Elementos de botiquines con fecha de vencimiento expirada
- Elementos que usan baterías sin carga activa
- Las sillas de ruedas existentes en la mayoría de los pisos de la sede principal, no cuentan con señalización ni demarcación a piso para tal fin.
- Extintores sin señalización, con obstáculos a su alrededor o sin soporte a piso
- Falta de camilla o con daños
- Botiquines incompletos, ausencia de solución salina
- Bodega sin alarma sonora ni escaleras de emergencia.

La OCI identifica una oportunidad de mejora encaminada a analizar la viabilidad y pertinencia para que se registren los planes de mejoramiento generados resultado de las diferentes evaluaciones desarrolladas al sistema, dando aplicabilidad al procedimiento Gestión del Plan de Mejoramiento (S-PD-005), cuyo objetivo se enmarca en *"Definir las acciones necesarias para corregir, prevenir o reducir los efectos no deseados, así como eliminar las causas de las no conformidades, provenientes de las diferentes fuentes, con el propósito de fortalecer la gestión de la Secretaría Distrital de Planeación mediante la mejora del desempeño de los procesos y prestación de los productos y/o servicios."* (Subrayado fuera del texto). Lo anterior, por cuanto las acciones que haya ejecutado la Dirección de Talento Humano para subsanar las debilidades detectadas, no están siendo parte del proceso de mejoramiento continuo establecido en la entidad, careciendo de monitoreo y seguimiento por parte de la segunda y tercera línea de defensa (Dirección de Planeación Institucional y Oficina de Control Interno), sin desconocer los seguimientos que realice en su rol la Dirección de Talento Humano.

4.3.17 RIESGOS AMBIENTALES

Conforme a lo establecido en el Plan Institucional de Gestión Ambiental 2020-2024 A-LE-023, La política ambiental de la Secretaria Distrital de Planeación instaura que *"La Secretaria Distrital de Planeación se compromete a responder por las políticas territorial, económica, social, ambiental y cultural del Distrito Capital, en el marco de sus competencias para garantizar el crecimiento ordenado, el mejor aprovechamiento del territorio y la equidad e igualdad de oportunidades para sus habitantes, con un equipo humano competente, cumpliendo con las disposiciones legales aplicables y los requisitos de los usuarios y partes interesadas, mediante la sostenibilidad y el mejoramiento continuo del Sistema Integrado de Gestión así como el cumplimiento de la siguientes directrices ambiental: La Secretaria Distrital de Planeación se compromete con la promoción de la conciencia ambiental en los servidores, el uso eficiente de los recursos naturales y la gestión adecuada de los aspectos ambientales significativos en la operación de la entidad*."

Por otra parte, la entidad identifica Aspectos Ambientales (A/A) que son los elementos de las actividades propias de la Secretaría Distrital de Planeación que pueden interactuar con el Ambiente, que tiene un efecto o impacto ambiental significativo y su valoración ambiental. En relación con lo anterior para la valoración de los aspectos ambientales, la entidad encontró varios impactos significativos por cada aspecto ambiental, con mayor relevancia que son:

- La generación de residuos
- Consumo de agua.
- Consumo de Energía Eléctrica

Conforme a lo anterior, la Oficina de Control Interno indagó a la Dirección Administrativa sobre la actualización del Plan Institucional de Gestión Ambiental - A-LE-023, dado que el registrado corresponde a 2021, quien informó que no se han efectuado actualización al Plan institucional de Gestión Ambiental en espera de dar cumplimiento al mismo en la vigencia 2024, para reportar el cuatrienio y no se han identificado riesgos adicionales.

Para la elaboración del presente informe, la Oficina de Control Interno verificó las evidencias reportadas a los seguimientos de los riesgos así:

Riesgo ID-183 Manejo y gestión inadecuada de residuos sólidos

Este riesgo se presenta con una tipología Operativo – Ambiental y reporto el siguiente seguimiento, de acuerdo con el Plan de Acción del PIGA, planteado para el año 2020 - 2024, al Plan de Acción Interno para el Manejo de Residuos Convencionales y Peligrosos.

1. Se realizó el pesaje y el consolidado mensual de los residuos generados por la Secretaria Distrital de Planeación.
2. Se gestionó y realizó con Puerta de Oro destrucción documental en archivo
3. Se organizó capacitación presencial al equipo de aseo y cafetería sobre disposición adecuada de residuos_2023.
4. Se clasificaron, rotularon y almacenaron residuos peligrosos: luminarias, cartuchos y tóneres, en la primera jornada de la Reciclatón organizada por la Secretaría Distrital de Ambiente.
5. Se realizó la inspección al centro de acopio del CAD, se realizó acompañamiento a las respectivas entregas al operador de residuos aprovechables.
6. Se adelanto el informe sobre Plásticos de un solo uso y su respectiva inclusión en el contrato de Aseo y Cafetería.
8. Se gestionó con UAESP y Secretaría de Ambiente se realizó para adelantar la agenda de la Semana Ambiental
9. Se promovió la contratación y el clausulado sostenible mediante talleres de prácticas empresariales
10. Se fortalecieron capacidades conceptuales en términos de cambio climático
11. Se llevan a cabo los balances para variables de consumo para energía y agua, así como los pesajes de los residuos sólidos.

Se verificaron los siguientes soportes para los residuos sólidos tanto ordinarios como peligrosos, para los cuales se realizaron talleres (consumo responsable, economía circular, descomposición de residuos, de consumo responsable, entre otros) capacitaciones, piezas para el reciclaje de (botellas, cartón, latas, plásticos y su separación por colores), a su vez acuerdos de corresponsabilidad, los cuales corroboran las actuaciones realizadas por la dirección administrativa con el fin de minimizar o mitigar estos riesgos se recomienda contemplar seguimientos asociados al transporte y al manejo inadecuado o manipulación de estos residuos peligrosos.

Riesgo ID-184 Uso ineficiente de los Recursos (Agua y Energía)

Este riesgo se presenta con una tipología Operativo – Ambiental y reporto el siguiente seguimiento

1. Se realizó bimestralmente un consolidado del consumo de agua en las instalaciones de la entidad.
2. Se realizó bimestralmente un consolidado del consumo de energía en las instalaciones de la entidad.
3. Se realizó una inspección a las instalaciones de las sedes de la entidad, con el fin de identificar el buen funcionamiento las redes hidrosanitaria y eléctrica
4. Se realizó Campaña – Ahorra agua, ahorra energía y ahorra papel

Se verificaron los siguientes soportes para el uso eficiente del agua como capacitaciones de ahorro de agua, seguimientos al consumo de agua, inventarios de sistemas hidrosanitarios y socializaciones sobre el consumo de agua y energía. Por otra parte, se realizaron capacitaciones de ahorro de energía, infografías de energías renovables, gestión eficiente energía en entidades y cinco tips para ahorro de energía, entre otros, socialización del consumo de energía, y seguimiento a dichos consumos, los cuales corroboran las actuaciones realizadas por la dirección administrativa con el fin de minimizar o mitigar estos riesgos.

Por otra parte, se verificó la matriz de impactos 242 tanto para el consumo de agua como de energía conforme a lo señalado en La Resolución 242 de 2014 emitida por la Secretaría Distrital de Ambiente, en donde se establecieron los lineamientos para la formulación, concertación, implementación, Evaluación, Control y Seguimiento Ambiental de los Planes Institucionales de Gestión Ambiental – PIGA para lo cual se identifican.

Para el Consumo de Agua desarrolla actividades asociadas al aspecto como:

- Mantenimiento y limpieza de la infraestructura física,
- Actividades asociadas al uso sanitarios,
- Actividades asociadas al uso lavamanos y
- Tareas de revisión y control de pérdidas de agua

Con un Impacto ambiental de Agotamiento de los Recursos Naturales con una Probabilidad (ALTA) Es muy posible que suceda en cualquier momento, con una Magnitud o calificación (MODERADA) Alteración moderada del recurso, tiene un potencial de riesgo medio sobre el ambiente y finalmente presenta controles operacionales como:

- Seguimiento bimestral del consumo de agua.
- Inspecciones trimestrales a las instalaciones hidrosanitarias de la entidad.
- Una (1) capacitación sobre uso eficiente y racional del agua.
- Recibos de Pago de agua de la sede de archivo.
- Relación consumos sede CAD (pro rateada). Línea base consumo agua
- Inspecciones trimestrales a las instalaciones hidrosanitarias de la entidad

A su vez, para el consumo de energía eléctrica desarrolla actividades asociadas al aspecto como:

- Uso de equipos (computadores, impresoras)

- Uso de redes eléctricas (iluminación)
- Uso de herramientas para mantenimientos locativos

Con un Impacto ambiental de Agotamiento de los Recursos Naturales con una Probabilidad (MEDIA) Existe una posibilidad media que suceda, con una Magnitud o calificación (MODERADA) Alteración moderada del recurso, tiene un potencial de riesgo medio sobre el ambiente y finalmente presenta controles operacionales como:

- Seguimiento bimestral del consumo de energía.
- Una (1) capacitación sobre uso eficiente y racional de la energía.
- Inspecciones trimestrales a las instalaciones de la red eléctrica.
- Sistemas ahorradores de energía (Led, equipos con eficiencia energética).
- Línea base consumo de energía.
- Recibos de Pago de energía de la sede de archivo.
- Relación consumos sede CAD (pro rateada)

Se recomienda fortalecer los controles identificados y asociarlos con el tema del calentamiento global o cambio climático y sus consecuencias con el razonamiento de agua que se presenta actualmente.

4.3.18 Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo SARLAFT

Para el seguimiento de este Sistema, la Oficina de Control Interno solicitó que de acuerdo con el E-IN-111 MANUAL SARLAFT Versión 2 de febrero de 2024, la Secretaría Distrital de Planeación cuenta con un período máximo de 10 meses para implementar la política, lineamientos, metodologías y procedimientos incluidos en este manual.

En cuanto a los avances en la implementación en la entidad, la Dirección de Planeación Institucional informó que *"los planes de aplicabilidad del Manual SARLAFT fueron diseñados por la Dirección de Planeación Institucional, la Dirección de Contratación y la Dirección de Talento Humano, como líderes responsables de la implementación de estos lineamientos. Con corte a mayo de 2024 se ha avanzado en la implementación de los planes de aplicabilidad, obteniendo un avance del 61,43% de las acciones a cargo de la Dirección de Planeación Institucional, el 23,03% para las actividades a cargo de la Dirección de Talento Humano y 19,56% para las acciones a cargo de la Dirección de Contratación, logrando un avance ponderado del 34,67%. Por otra parte, vale la pena aclarar que algunas de las actividades de los planes tienen fecha de finalización a diciembre de 2024 porque corresponden a tareas periódicas, es decir, se implementa el lineamiento y se continúa desarrollando la actividad durante la vigencia. Se estipuló de esta forma porque los planes de aplicabilidad también hacen parte del Plan anticorrupción y de atención al ciudadano alineado con los Programas de transparencia y ética pública, lo cual contribuye al cumplimiento de la ley 2195 de 2022."*

Conforme a lo anterior, se contrastaron los Soportes enviados así:

La dirección de Planeación Institucional presenta un cronograma con corte a 31 de mayo del presente año, con 21 actividades de las cuales se verificaron en el aplicativo SIPA la incorporación y publicación de los siguientes formatos E-FO-117 *Reporte detallado de consultas SARLAFT*, E-FO-119 *Reporte de operaciones inusuales*, E-FO-116 *Control de operaciones inusuales y sospechosas*, E-FO-115 *Identificación de PEP'S persona natural*, E-FO-114 *Identificación de PEP'S persona jurídica*, E-FO-120 *Base de datos PEP´s*, E-FO-118

Conocimiento/actualización de persona jurídica, E-FO 121 *Formato del Mapa de riesgo SARLAFT.*

Por otra se encuentra pendiente de publicar los formatos de los procedimientos de "*Consulta de listas y fuentes de información pública", "Gestión de operaciones inusuales y sospechosas" y "Gestión de PEP's en la SDP"* para los cuales presentan un avance del 50% y 80% respectivamente, a su vez pendiente de revisar y ajustar las tablas de retención documental con la Dirección Administrativa.

La Dirección de Planeación Institucional creó un Drive para archivar información relacionada con el SARLAFT y solicitó a la Dirección de Tecnología de la Información y las Comunicaciones, la periodicidad del Backup de la información del drive del SARLAFT.

A su vez presenta actividades de socialización e instrumentos de divulgación del SARLAFT al interior de la entidad. Finalmente, para la para el segundo semestre del año se tienen programadas las siguientes actividades:

- Crear la estructura del informe anual de reporte del SARLAFT ante el Comité Institucional de Coordinación de Control Interno (CCCI)
- Socializar el Procedimiento Gestión de operaciones inusuales y sospechosas
- Revisar en la vigencia 2024 con la Secretaria General el registro del Oficial de Cumplimiento de la SDP en la UIAF, si van a gestionarla ellos para todas las Entidades del distrito (como lo dijeron en sesión de la ROC de 2023) o cada Entidad debe adelantar esta actividad de forma independiente y gestionar el registro
- Generar los reportes pertinentes a la UIAF una vez se habiliten las opciones / funcionalidades por parte de esta entidad.

La Dirección de Contratación presenta un cronograma con 18 actividades y avances en 7 actividades con un porcentaje total de 19.56%. Las demás actividades según cronograma en el plan de aplicabilidad para los lineamientos del manual SARLAFT, corresponden al segundo semestre del año 2024. Se verificaron las evidencias reportadas según las actividades desarrolladas así:

1. Implementar que, en los procesos competitivos de selección de la entidad, en los pliegos de condiciones o en sus equivalentes, se establezca como requisito jurídico verificar a los Proponentes que ocupen hasta el tercer orden de elegibilidad, adelantaron procesos de convocatoria pública a los cuales se les incluyó dentro de la Invitación Pública y/o Anexo General de Especificaciones.

   Invitación Publica (Mínima Cuantía): Numeral 14,1,9. Otros documentos del proponente (adjunto pantallazo)

- El proponente deberá allegar junto con su propuesta la autorización para la consulta DEL Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT) (Formatos Adjuntos a la invitación" E-FO- 113 y E-FO-115). En caso de que el proponente sea persona jurídica deberá además diligenciar el anexo E-FO-118 (Estos documentos deberán marcarse con carácter de confidencial) en la plataforma SECOP II

14.2. Requisitos técnicos:

14.2.1 Experiencia del proponente (persona natural y jurídica):

Para el presente proceso el proponente debe adjuntar hasta DOS (2) certificaciones de experiencia, expedidas por el contratante a nombre del proponente o alguno(s) de los integrantes del consorcio o unión temporal proponente, sobre contratos EJECUTADOS a más tardar a la fecha definitiva del plazo para presentar ofertas, inclusive, cuyo objeto, obligaciones, alcance o condiciones sean similares al objeto del presente proceso. La sumatoria del valor de las certificaciones debe ser igual o superior al valor del presupuesto oficial asignado del presente proceso.

Las certificaciones deben contener:

1. Nombre o razón social del contratante.
2. Nombre e identificación del contratista.

Anexo General de Especificaciones (Otras Modalidades):
Concurso de Méritos
Numeral 14,1,9. Otros documentos del proponente:

Documentos de la oferta

Los siguientes documentos deben ser presentados con la oferta.

Sobre: Sobre único

Descripción	Año	Periodo
EL PROPONENTE DEBERÁ ALLEGAR EL ANEXO 1 CARTA DE PRESENTACIÓN SUSCRITA POR EL REPRESENTANTE LEGAL		
• El proponente deberá allegar junto con su propuesta los formatos DILIGENCIADO EFO 114 Y EFO 118 AUTORIZANDO A LA ENTIDAD LA VERIFICACION EN SARLAFT - PARA LA ADJUDICACION (estos documentos no son objeto de evaluacion)		
• El proponente deberá allegar junto con su propuesta el certificado de Deudores Alimentarios Morosos – REDAM, del Representante Legal, con una vigencia no superior a 30 dias.		

SELECCIÓN ABREVIADA - MENOR CUANTÍA
2.1.10. Verificación SARLAFT

2.1.10. Verificación SARLAFT

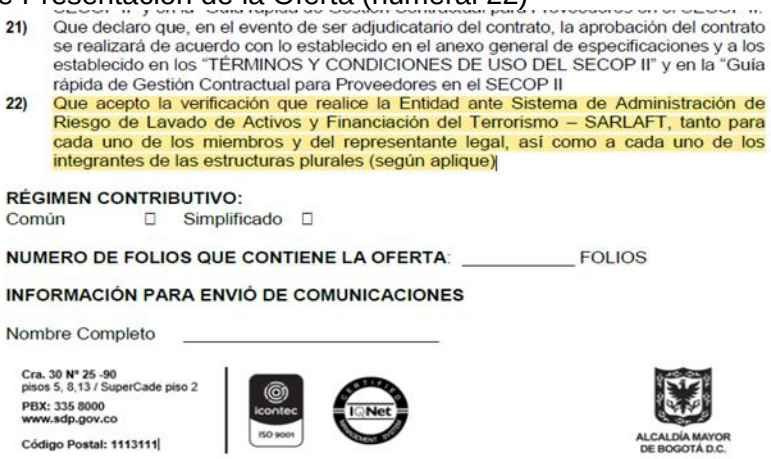
La Entidad verificara a los Proponentes que ocupen hasta el tercer orden de elegibilidad, la culminación satisfactoria de las verificaciones que se adelanten en el marco de los lineamientos del SARLAFT de la Entidad, las cuales se desarrollarán conforme a las disposiciones legales y reglamentarias respecto de los proponentes (persona natural y jurídica), para cada uno de sus miembros y su representante legal, así como a cada uno de los integrantes de las estructuras plurales.

2.1.11. Otros documentos del proponente:

- El proponente deberá allegar junto con su propuesta el Certificado de Antecedentes Disciplinarios del proponente, expedido por la Procuraduría General de la Nación. Si el **proponente es persona jurídica**, se deberá allegar este documento tanto para el representante legal como para la empresa. No obstante, lo anterior, el **DISTRITO CAPITAL –SDP-** realizará la respectiva consulta.

2. Implementar que dentro de los modelos de carta de presentación de las ofertas de los procesos competitivos se incluya la autorización del proponente para realizar la verificación SARLAFT en el anexo general de especificaciones (otras modalidades):

SELECCIÓN ABREVIADA - MENOR CUANTÍA
Anexo 1 Carta de Presentación de la Oferta (numeral 22)



21) Que declaro que, en el evento de ser adjudicatario del contrato, la aprobación del contrato se realizará de acuerdo con lo establecido en el anexo general de especificaciones y a los establecido en los "TÉRMINOS Y CONDICIONES DE USO DEL SECOP II" y en la "Guía rápida de Gestión Contractual para Proveedores en el SECOP II

22) Que acepto la verificación que realice la Entidad ante Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT, tanto para cada uno de los miembros y del representante legal, así como a cada uno de los integrantes de las estructuras plurales (según aplique)

RÉGIMEN CONTRIBUTIVO:
Común ☐ Simplificado ☐

NUMERO DE FOLIOS QUE CONTIENE LA OFERTA: _____ FOLIOS

INFORMACIÓN PARA ENVIÓ DE COMUNICACIONES

Nombre Completo _____

Cra. 30 N° 25 -90
pisos 5, 8,13 / SuperCade piso 2
PBX: 335 8000
www.sdp.gov.co

Código Postal: 1113111

ALCALDÍA MAYOR DE BOGOTÁ D.C.

3. Implementar la solicitud del formato Identificación de PEP´s persona natural y jurídica y el reporte al Oficial de Cumplimiento, Se verificó el formato AFO-185 solicitud para contratar prestaciones de servicios profesionales y de apoyo a la gestión en el cual se incluyó dentro de los documentos soporte el formato de identificación PEP´s (persona natural o jurídica, según corresponda) (Decreto 830/2021) (E-FO-114 / e-fo-115)

4. solicitar el diligenciamiento del "formato de conocimiento y actualización de persona jurídica", para los casos que aplique, e identificar los beneficiarios finales, se verificó el formato afo-185 solicitud para contratar prestaciones de servicios profesionales y de apoyo a la gestión en el cual se incluyó dentro de los documentos soporte el formato de conocimiento y actualización de persona jurídica (E-FO-118) cuando aplique.

5. Implementar y realizar durante la vigencia la solicitud al Oficial de Cumplimiento de la consulta en listas restrictivas, vinculantes y fuentes de información pública a las personas que se van a contratar, dentro de las actividades relacionan que durante el I trimestre se adelantaron 448 consultas de listas restrictivas, vinculantes y fuentes de información pública asociadas a procesos de contratación que han adelantado las dependencias de la Secretaría, durante los meses de abril y mayo se han adelantado 72 consultas de listas restrictivas, vinculantes y fuentes de información pública . La información reposa en el drive SARLAFT y se adjunta una muestra de 3 consultas, por parte del grupo auditor se verificó estas muestras, donde se comprueba las solicitudes y resultados de estas consultas.

6. Implementar una cláusula en las obligaciones generales de los contratos sobre el cumplimiento de la política y lineamientos asociados al SARLAFT de la SDP, se verificó conforme las evidencias reportadas la inclusión en las minutas contractuales la obligación general #12 con dicho cumplimiento.

CONTRATO No. 236 de 2024

Tributario, el Decreto Nacional 1625 de 2016 "Único Reglamentario en Materia Tributaria" y las normas que le modifican o adicionan. Lo anterior, en cumplimiento de lo ordenado por la Ley 2013 de 2019 y la Circular conjunta No. 001 de 2020 expedida por la Secretaría General de la Alcaldía Mayor de Bogotá y el Departamento Administrativo del Servicio Civil Distrital. Esta constancia también será verificada en el último pago, como soporte para suscribir el acta de recibo final del contrato). **12)** Dar cumplimiento a la Política y Lineamientos asociados al Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo - SARLAFT establecidos en el Manual de la SDP (E-IN-111). **13)** Realizar la actualización y reporte de la Declaración de Bienes y Rentas y Conflicto de Interés en el aplicativo SIDEAP, de conformidad con los lineamientos distritales y en el término que el DASCD establezca en la respectiva vigencia, siempre y cuando el contrato se encuentre en ejecución en la fecha establecida para actualización anual.

TERCERA.- PROTECCIÓN DEL SOFTWARE: En el evento en que para el desarrollo del objeto contractual el **CONTRATISTA** requiera utilizar equipos o software del **DISTRITO CAPITAL -SDP-**, deberá observar las siguientes reglas: **1)** No instalar software sin la autorización previa y escrita del

7. Solicitar al Oficial de cumplimiento la consulta en listas y fuentes de información pública de las novedades de cesión de contratos, para lo cual se implementó la solicitud de consulta para cesiones de contratos, se han realizado 6 cesiones de contrato con la consulta SARLAFT, se evidencio la consulta de 4 cesiones que se reportaron como muestra de esta actividad para los contratos 018 con reporte 186, 060 con reporte 232, 103 con reporte 267 y 446 con reporte 256 de 2024.

Es así, como se presenta 10 actividades a cargo de la Dirección de Talento Humano, con avances que corresponden al 23%. Las otras cinco actividades faltantes y reportadas en cronograma del plan de aplicabilidad de lineamiento manual SARLAFT, corresponden al segundo semestre de 2024. Se verificaron las evidencias reportadas según las actividades desarrolladas así:

1. Socializar la actualización del Código de integridad y Código de Buen Gobierno a los funcionarios de la Secretaría, se evidencian 5 reuniones con los gestores de integridad y María Auxiliadora de la Hoz, los días 19 de enero, 19 de febrero, 20 de marzo, 22 de abril y 16 de mayo de 2024, donde se ha revisado el Plan de integridad y se está trabajando en la propuesta de estrategia de comunicaciones para la socialización del código de integridad y el código de buen gobierno. Por otra parte, se adjunta formato A-FO-184 control de reuniones y presentación con los lineamientos SARLAFT en el código de integralidad.
2. Incluir el formato de Identificación de PEP´s en el proceso de vinculación y remitirlo al Oficial de Cumplimiento, se evidencia como muestra cinco formatos E-FO-115 Identificación PEP´s persona natural, a su vez el formato A-FO-530 Autorización Tratamiento de Datos Personales debidamente diligenciados y firmados para los meses enero, febrero, marzo abril y mayo de 2024, y cuadro de seguimiento SARLAFT para 55 funcionarios vinculados
3. Implementar la solicitud de consulta de listas restrictivas, vinculantes y fuentes de información pública en la etapa de ingreso de funcionarios, se verifico las evidencias reportadas con el formato E-FO- 113 Solicitud de Consultas SARLAFT Persona Natural para la consulta en listas restrictivas, vinculantes y fuentes de información pública, para los cinco primeros meses del año con su respectivo correo de solicitud y cuadro de seguimiento SARLAFT para 55 funcionarios vinculados.
4. Implementar y realizar durante la vigencia las solicitudes al Oficial de cumplimiento de consulta de listas restrictivas, vinculantes y fuentes de información pública cuando se retiren los funcionarios, se evidencian cinco muestras de consultas de funcionarios retirados según formato E-FO- 113 Solicitud de Consultas SARLAFT Persona Natural de los 25 funcionarios

que se han retirado de la Secretaría a la fecha, con su respectivo correo de solicitud y cuadro de seguimiento SARLAFT.

5. Definir los cargos de la SDP que ostentan la condición de PEP's e Implementar y reportar durante la vigencia al Oficial de cumplimiento las novedades de retiro de funcionarios que sean PEP's para actualizar la base de datos de PEP´s de la SDP, esta actividad refleja un avance del 10% se evidencia pantallazo de la reunión realizada el 24 de mayo para revisar el concepto del DASC y definir como se desarrollará el trabajo para identificar los funcionarios que son PEP's en la SDP, comunicación por parte de la dirección jurídica en respuesta sobre solicitud de concepto viabilidad de registro de -PPE en -SIDEAP.

Finalmente, en el Plan de aplicabilidad, no se registran actividades conforme a la Metodología de Implementación de Gestión del Riesgo SARLAFT capítulo 6 del Manual E-IN-111, tales como la identificación de los riesgos, la valoración de los riesgos con su análisis, evaluación, definición y valoración de los controles y los planes de tratamiento para reducir el riesgo, el monitoreo y actualización de estos riesgos de SARLAFT.

5. Fortalezas

La disposición mostrada por el equipo de la Dirección de Planeación Institucional, así como la Dirección Administrativa, Dirección de Talento Humano y la Dirección de Tecnologías de la Información y las Comunicaciones en el seguimiento.

Se evidencia la actualización de los diferentes mapas de riesgos tanto de gestión, corrupción y de seguridad de la información, contemplando los planes de acción para la vigencia 2024 con el fin de darle un tratamiento (reducir o mitigar) los riesgos identificados conforme a lo establecido en la Política de administración de riesgos.

La entidad se encuentra implementando el sistema de Riesgo de Lavado de Activos, Financiación del Terrorismo SARLAFT contemplando lineamientos para el diseño de planes de aplicabilidad del manual al interior de la Secretaria Distrital de Planeación.

6. Situaciones susceptibles de mejora / oportunidades (observaciones)

N°	Descripción de situación susceptible de mejora / oportunidades (observación)	Numeral del informe Capítulo 4	Responsable
1.	Se evidencia que todos los riesgos residuales de corrupción, sin excepción, permanecen en el mismo nivel que los inherentes, pese a que se están administrando 56 controles. Lo anterior es una señal de alerta toda vez que el 83% de los riesgos están en los niveles extremo y alto, aunque se gestionen sus controles.	4.2.2.2	Dirección de Planeación Institucional
2.	De acuerdo con lo señalado en el numeral 4 del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (A-LE-505) para la vigencia 2024, la actualización de instrumentos, de activos de información, aprobación de activos de información y publicación de los instrumentos (registros de activos de información e índice de información clasificada y reservada) se tenía prevista entre febrero y abril de 2024. Sin embargo, el documento Registro de Activos de Información (RAI)	4.2.2.3	Dirección de Tecnologías de la Información y las Comunicaciones

N°	Descripción de situación susceptible de mejora / oportunidades (observación)	Numeral del informe Capítulo 4	Responsable
	(A-LE-283) presenta en el SIPA su versión 11 de octubre de 2022, sin evidenciar la actualización que trata el A-LE-505.		
3.	Para los riesgos de Seguridad de la Información por proceso, no fue posible establecer o comparar el riesgo residual con el riesgo inherente, ya que no se observa una Evaluación del Riesgo - Nivel del Riesgo Residual unificada por cada riesgo, dado que se determina es por cada control.	4.2.2.3	Dirección de Tecnologías de la Información y las Comunicaciones
4.	Del análisis efectuado a los riesgos de gestión, corrupción y seguridad de la información por cada proceso de la entidad, se evidenciaron oportunidades de mejora que se registran detalladamente en el cuerpo del informe y que se refieren principalmente a: • Mejorar la redacción de los riesgos que permita identificar claramente sus elementos y de fácil entendimiento a todos los niveles de consulta • Profundizar en el análisis de causas definidas como la ausencia de copias de respaldo, desconocimiento, entre otros. • Algunas causas son resultado de otras causas, y en algunos casos se incluyen consecuencias. • En algunos casos no fue posible establecer relación directa entre las causas y los controles estructurados. • La asistencia a capacitaciones desdibuja la realidad de un control que permita reducir o mitigar el riesgo, sin desconocer que pueden aportar a la mejora. • En cuanto al objetivo de control y el control en los riesgos de seguridad de la información, en algunos casos no hay relación entre el objetivo control y la actividad de control • En la descripción de algunos controles no se evidencia la frecuencia o la periodicidad con la que se realiza o ejecuta la actividad. • En algunos controles, no se registra el Propósito del control y no se aporta descripción de la evidencia resultante una vez ejecutado el control, solo se atribuye variable de que cuenta con registro, lo cual no es diciente al momento de la evaluación. • Se ha evidenciado materialización de riesgos documentadas en los informes de auditorías, seguimientos y evaluaciones internas y externas de que han sido objeto los procesos en la entidad, sin que se observe la documentación de estos hechos. • Algunos activos de información no pudieron ser identificados en el A-LE-283 Registro de Activos de Información (RAI) y/o no correspondían a activos calificados con criticidad Alta, según lo establecido en la Política de Administración del Riesgo E-LE-030	4.3	Líderes de Proceso Dirección de Planeación Institucional
5.	Del reporte de incidentes dentro del Sistema de Seguridad y Salud en el Trabajo, se observa el diligenciamiento del formato de investigación de incidentes, accidentes laborales y enfermedad de origen laboral SDP (A-FO-402), sin las firmas de	4.3.12	Dirección de Talento Humano

N°	Descripción de situación susceptible de mejora / oportunidades (observación)	Numeral del informe Capítulo 4	Responsable
	los intervinientes por parte de seguridad y salud en el trabajo, accidentado, jefe inmediato y COPASST, siendo esto esencial para la autenticidad, formalización, oficialización y salvaguarda de los documentos como soportes de las investigaciones. Adicionalmente, en los campos Jefe Inmediato y COPASST no se presentan los nombres respectivos.		
6.	En el plan de aplicabilidad del Manual del Sistema de Administración del Riesgo de Lavado de Activos y Financiación al Terrorismo (SARLAFT) no se registran actividades conforme a la Metodología de Implementación de la Gestión del Riesgo SARLAFT capítulo 6 del Manual, tales como la identificación de los riesgos, la valoración de los riesgos con su análisis, evaluación, definición y valoración de los controles y los planes de tratamiento para reducir el riesgo, el monitoreo y actualización de estos riesgos de SARLAFT.	4.3.18	Dirección de Planeación Institucional
La formulación de planes de mejoramiento es opcional para las situaciones de mejora identificadas, no obstante, la Oficina de Control Interno - 4OCI revisará las medidas adoptadas en la próxima auditoría y/o seguimiento.			

7. Situaciones críticas

N°		Reincidente (si/no)	
Descripción de la situación crítica			
Criterio Incumplido (Estándar/norma/reglamento)			
Numeral del informe (capítulo 4)			
Responsable			
Posible efecto			
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)			

8. Recomendaciones

En la Política de Administración del Riesgo (E-LE-030) incluir la integralidad de los riesgos por tipología como Continuidad del negocio, Contingentes, Legales, Lavado de Activos y Financiación del terrorismo SARLAFT, Seguridad y Salud en el Trabajo, Ambientales y Fiscales.

Establecer un mecanismo que permita el reporte de la materialización de los riesgos de forma oportuna con el fin de realizar la gestión necesaria para su tratamiento.

Fortalecer la planificación de la Gestión del Cambio en la entidad, a fin de disminuir los impactos negativos que se puedan generar por su implementación, atendiendo lo establecido en el numeral 6.3 de la norma NTC ISO 9001:2015 y el procedimiento *Identificación, implementación y seguimiento de la gestión del cambio* E-PD-025.

Actualizar el mapa de riesgos institucional (E-LE-017) publicado en el SIPA conforme los ajustes realizados por cada uno de los procesos en los mapas de riesgos.

Revisar y ajustar la clasificación de los controles catalogados como correctivos, para aquellos que no se relacionan con la gestión en el evento de una materialización de riesgos, igualmente, fortalecer los controles sin registro a fin de documentarlos.

Almacenar la documentación que soporta la gestión del cambio en formatos que no permitan su modificación, una vez sean aprobados por instancias decisorias de la entidad, atendiendo a que los formatos suministrados se encontraban en archivos Word.

Revisar los riesgos de corrupción y los controles establecidos para su tratamiento, considerando necesario tener en cuenta, entre otros:

- Si hay deficiencias en aplicación de la metodología
- Si el impacto que tienen los controles sobre el riesgo no es lo suficientemente contundente, o
- Si los controles existentes son insuficientes.

Identificar los posibles riesgos de corrupción asociados a los Trámites y Otros Procedimientos Administrativos –OPAS, en concordancia con lo establecido en el *Protocolo para la identificación de riesgos corrupción asociados a la prestación de trámites y servicios* del Departamento Administrativo de la Función Pública.

Incluir para los riesgos de corrupción los atributos de eficiencia para el diseño de los controles el interrogante sobre si la implementación de los controles se realiza de forma automática o manual, conforme a lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

Revisar las respuestas dadas en la Valoración de los Controles a los Riesgos de Corrupción para que se ajuste a la realidad en la ejecución de éstos.

Atender lo indicado en el Informe de Auditoría de Sistemas de Gestión de Icontec, respecto de *"reconsiderar el "desconocimiento" como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos."*

Establecer las acciones que permitan cumplir con lo programado en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (A-LE-505) para la vigencia 2024 y generar una versión actualizada de los activos de información acorde con la realidad de la entidad.

Revisar y ajustar los mapas de riesgos de seguridad de la información, a fin de que el método de valoración del riesgo Inherente (por riesgo o por combinación amenaza – vulnerabilidad) metodológicamente corresponda de igual manera al riesgo residual con promedio ponderado tomando todos los controles, en donde se evidencie el desplazamiento que tendrá el riesgo al evaluar el diseño de los controles.

Para los mapas de riesgos de seguridad de la información es importante que, el método de valoración del riesgo Inherente corresponda al riesgo residual en donde se evidencie claramente el desplazamiento que tendrá el riesgo al evaluar el diseño de los controles.

Fortalecer los controles, atendiendo las características de un control (responsable, periodicidad, propósito, evidencia) definidas en la Política de administración del riesgo y la Guía para la

administración del riesgo y el diseño de controles en entidades públicas en su versión 4.

Revisar los controles catalogados como correctivos en los diferentes mapas de riesgos, para que se ajusten a su definición en la política de administración del riesgo *"ataca el impacto cuando el riesgo ya se ha materializado. El control se acciona posterior a la ejecución del proceso o actividad y ya se han presentado las consecuencias."*.

Para los Grupos de Exposición Similar – GES, se sugiere la revisión de la información registrada a fin de que los contratistas sean incluidos en las actividades del grupo a los que sean asignados dichos niveles.

Evaluar la valoración de las situaciones relacionadas con eventos deportivos, atendiendo que se presentaron varios accidentes de trabajo relacionadas con estas actividades.

Fortalecer el Plan de Capacitación Anual del Sistema de Seguridad y Salud en el Trabajo (SSST) para que se visibilicen variables como cantidad de capacitaciones programadas, fechas previstas, población objetivo, entre otros, que permitan realizar seguimiento del cumplimiento de las actividades propuestas a nivel de todas las líneas de defensa. Además, se sugiere que para la programación de este plan se tengan en cuenta los resultados de las mediciones realizadas sobre el sistema como insumo que propenda por la efectividad de las capacitaciones programadas, así como establecer mecanismos efectivos que incentiven la participación de los funcionarios y contratistas.

Establecer mecanismos de control que permitan reflejar información coincidente en los diferentes instrumentos de reporte de información del SSST y se ajusten a la realidad de las actividades desarrolladas en la entidad.

Registrar los planes de mejoramiento generados resultado de las diferentes evaluaciones desarrolladas al SSST, dando aplicabilidad al procedimiento Gestión del Plan de Mejoramiento (S-PD-005), por cuanto las acciones que ejecutadas por la Dirección de Talento Humano para subsanar las debilidades detectadas no están siendo parte del proceso de mejoramiento continuo establecido en la entidad, careciendo de monitoreo de la segunda línea de defensa y seguimiento de la tercera línea, al igual para aquellos indicadores del SSST que no alcanzan su cumplimiento, establecer planes de mejoramiento como una herramienta de mejora.

Fortalecer la identificación de los controles de los riesgos ambientales y asociarlos con el tema del cambio climático y sus consecuencias como el razonamiento de agua que se presenta actualmente.

Nombres / Equipo Auditor	
Auditor líder	Iván Fernando Tunjano Reyes
Auditor(es)	Johana Milena Pulido Montañez

Denis Parra Suárez
Jefe Oficina de Control Interno