# INFORME EVALUACIÓN INDEPENDIENTE GESTIÓN DE RIESGOS VIGENCIA 2021

DIEGO MAURICIO ECHEVERRI ARANGO
Jefe de Oficina de Control Interno

BEATRIZ ELENA DUQUE ECHEVERRI
Profesional Universitario 1

LAURA RAMIREZ ARROYAVE
Auxiliar Administrativo

OFICINA DE CONTROL INTERNO

MEDELLÍN, NOVIEMBRE DE 2021

# TABLA DE CONTENIDO

**Pág.**

# LISTA DE TABLAS

Pág.

# LISTA DE GRÁFICOS

pág.

# 1. INTRODUCCION

La Oficina de Control Interno de la Contraloría General de Medellín, en cumplimiento de las funciones asignadas en la Ley 87 de 1993 y en virtud del rol de evaluación y seguimiento asignado a través del artículo 17 del Decreto 648 del 2017, realiza el presente informe de evaluación a la gestión de riesgos de la entidad con corte al 30 de octubre de 2021, teniendo en consideración los lineamientos del Departamento Administrativo de la Función Pública DAFP en el marco del Modelo Integrado de Planeación y Gestión MIPG y la Guía para la Gestión del Riesgo y el diseño de controles versión 5 de 2020.

Para el desarrollo de la presente evaluación, se realizó el estudio de la Guía para la Administración del Riesgo y el Diseño de Controles de la Función Pública, publicada en Diciembre de 2020; así como la documentación propia de la Entidad, entre otras, lo relacionado con la Política de Gestión de Riesgos y de Control Interno, toda vez que en ésta se establecen las responsabilidades de las diferentes Líneas de Defensa.

Posteriormente se realizó una evaluación de los lineamientos establecidos en la Política de Administración del Riesgo, de acuerdo con lo establecido en la Guía de la Función Pública identificando el cumplimiento de dichos lineamientos en la Política definida en la Entidad; adicionalmente se analizó lo relacionado con la Institucionalidad, con el fin de evidenciar las gestiones adelantadas por las diferentes Líneas de Defensa, de acuerdo con lo establecido en la Política de Control Interno y que está directamente relacionado con la Gestión del Riesgo.

En la evaluación, se analizó la aplicación de la metodología en la Entidad; para lo cual se realizó la revisión del mapa de riesgos, tanto de gestión, como de corrupción y de seguridad de la información; realizando un análisis de las diferentes etapas, conforme a la metodología establecida por la Función Pública; esto es la identificación y valoración del riesgo**.**

Por último, al final del informe se presentan consolidadas las conclusiones del trabajo realizado y una conclusión general, con la que se busca que en la Entidad se fortalezca la gestión de riesgos.

# 2. NORMATIVIDAD RELACIONADA

La Contraloría General de Medellín en cumplimiento a la política de Administración de Riesgos de la Entidad, la Guía de Administración de riesgos del DAFP versión 5, la ISO 9001:2015, los Lineamiento para la Administración de Riesgos, en pro del aseguramiento de los resultados institucionales y del mejoramiento continuo de la entidad, estableció el mapa de riesgos institucional para la vigencia 2021, en un trabajo articulado de la Oficina Asesora de Planeación y las diferentes dependencias de la Entidad.

Marco Legal:

- Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en la entidades y organismos del estado y se dictan otras disposiciones.
- Decreto Nacional 648 de abril de 2017 de la Presidencia de la República, por medio del cual se modifica y adiciona el Decreto Nacional 1083 de 2015.
- Ley 1474 de 2011, Estatuto Anticorrupción
- Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas, riesgos de Gestión, Corrupción y riesgos de Seguridad de la Información versión 5 de la Función Pública.
- ISO 9001:2015 Sistema de Gestión de la Calidad Requisitos
- Manual de Políticas de Operación de la Contraloría General de Medellín código M-GE-PL-002 versión 7
- Módulo de Riesgos Isolución

# 3. OBJETIVOS DE LA EVALUACION

## 3.1 OBJETIVO GENERAL

Verificar la efectiva implementación de la Gestión del riesgo en la Contraloría General de Medellín, entre otras, en lo relacionado con las fases de identificación y valoración de los riesgos, en el cual se incluye el diseño y la ejecución de los controles.

## 3.2 OBJETIVOS ESPECIFICOS

- Revisar que se tenga establecida la Política de Administración del Riesgo, que ésta cumpla con lo establecido en la Guía de Administración de Riesgos y que se esté dando cumplimiento a lo planteado en dicha política.

- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.

- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

- Revisar el perfil de riesgo inherente y residual para algunos procesos y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de

la entidad o que su calificación del impacto o probabilidad del riesgo no sea coherente con los resultados de las auditorías realizadas.

- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos

# 4. ALCANCE

La evaluación a la gestión de riesgos en la Contraloría General de Medellín, tendrá en cuenta la información generada durante la vigencia 2021.

# 5. METODOLOGIA

- Estudio de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, año 2020 de la Función Pública.

- Revisión y análisis documental de la Política de Operación, procedimientos, caracterización de los procesos, entre otros.

- Identificar los requisitos establecidos para la Gestión del Riesgo en la Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas, riesgos de Gestión, Corrupción y riesgos de Seguridad Digital versión 5 de la Función Pública.

- Realizar mesas de trabajo con los líderes de los procesos, con el fin de realizar un diagnóstico sobre la implementación de la gestión de riesgos.

- Verificación del estado de implementación del módulo de riesgos del aplicativo ISOLUCION

# 6. RESULTADOS DE LA EVALUACIÓN

De acuerdo con el Modelo Estándar de Control Interno para el estado colombiano, el Componente Administración del Riesgo, se define como el "*conjunto de elementos que le permiten a la entidad identificar, evaluar y gestionar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales*" y este componente se estructura a través de los siguientes Elementos de Control:

- Políticas de Administración del Riesgo
- Identificación del Riesgo
- Análisis y Valoración del Riesgo

Para efectos de dar cumplimiento al objetivo propuesto en la evaluación, se identificaran los requisitos establecidos para el componente Administración del Riesgo y los mismos se detallan a continuación:

## 6.1 POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DE RIESGOS

De conformidad con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 5, la Política de Administración de Riesgos, corresponde a una "*Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos*"; por lo anterior, luego de evaluar la Política de Administración de Riesgos aprobada en la Entidad, se pudo evidenciar lo siguiente:

- Por Resolución 203 del 19/12/2014, artículo 1, "*se actualiza la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública DAFP, con base en el documento que la sustituya o la modifique*"; sin que se evidencie resolución posterior que la modifique o que de manera explícita indique la adopción de la actualización de la Guía realizadas por la Función Pública durante las vigencias 2018 y 2020; sin embargo, conforme a lo expresado se entiende que al ser actualizadas las guías, las mismas quedan adoptadas en la Entidad.

Adicionalmente en la Resolución 203 del 19/12/2014, se "*adopta la política general de administración del riesgo para la Contraloría General de Medellín, o aquellas que las actualicen, sustituyan o modifiquen…*"; sin que se indique la manera en que se formalizaría su actualización, modificación o sustitución; siendo importante tener en cuenta que esta Resolución se encuentra vigente.

- En reunión del Comité Institucional de Coordinación de Control Interno, Acta 02 del 01/03/2021, se evidencia la aprobación de la Política de Administración de Riesgos; manifestando que "*fue formulada y elaborada por la oficina Asesora de Planeación de cara a la nueva guía Versión 5, publicada por el Departamento Administrativo de la Función Pública en el mes de diciembre. Dicha política fue remitida a todos los miembros a través de memorando 1565 del pasado 22 de febrero en el cual se les solicitaba que realizaran su respectivo análisis y revisión ya que iba a ser puesta en consideración para su aprobación en el presente comité; por lo tanto, pregunta si algún miembro tiene alguna duda al respecto. Sin que nadie manifestara alguna inquietud, la Dra. Diana Carolina procede a poner a consideración la política de administración del riesgo, frente a lo cual todos los miembros del comité manifestaron que leyeron el memorando con la política y que no tienen observaciones, por lo tanto emiten su aprobación";* lo anterior, permite evidenciar que se da cumplimiento a lo establecido en la Guía de Administración de Riesgos, en la cual se plantea que dicha Política, debe ser establecida por la Alta Dirección, con el liderazgo del representante legal y la participación del Comité Institucional de Coordinación de Control Interno.

- La Política de Administración de Riesgos, se encuentra incluida en el Manual de Políticas de Operación, Código: M-GE-PL-002, Versión 7, del 09/08/2021; evidenciándose su inclusión, conforme al Control de Cambios del Manual, el 04/03/2021.

- En la validación realizada a los elementos mínimos que debe contener la Política de Administración de Riesgos, conforme a la Guía para la Administración del riesgo y el Diseño de Controles en Entidades Públicas, Versión 5 de diciembre de 2020, se evidenciaron, entre otros, los siguientes aspectos:

  - ✓ **Objetivo:** En el cual se establece que se gestionaran los riesgos de gestión, corrupción y de seguridad de información; mediante la aplicación de la metodología definida por el DAFP.

- ✓ **Alcance:** De conformidad con la guía, se debe establecer *"…el ámbito de aplicación de los lineamientos, el cual debe abarcar todos los procesos de la entidad…*"; y al verificar en la Política aprobada, en ésta se plantea que: *"…El ámbito de aplicación de la Política de Administración de Riesgos, es sobre la Planeación Estratégica Institucional y los Procesos de la Entidad…*"; siendo consistente con lo establecido en la Guía.

  Adicionalmente, como parte del alcance, también se plantea que: "*para los procedimientos asociados a los procesos, el aseguramiento de los riesgos se hará mediante el establecimiento de puntos de control, en aquellas actividades criticas donde se establezca que hay riesgos para el cumplimiento de las mismas, los cuales no hacen parte del mapa de riesgos institucional*"; sin embargo, es importante tener en cuenta que los procedimientos, se encuentran definidos en la norma ISO 9000:2015, como la "*Forma especificada de llevar a cabo una actividad o un proceso*", siendo parte inherente de los procesos y con los cuales se da respuesta al requisito 4.4.1 de la norma ISO 9001:2015, el cual plantea que se deben "*…determinar los procesos necesarios para el sistema de gestión de la calidad y su aplicación a través de la organización…*"; y en el literal c), que se deben *"…determinar y aplicar los criterios y los métodos…*", entendidos éstos últimos como los procedimientos.

  No obstante lo anterior, la guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020, en el numeral 4.3.1, señala *"…algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos…";* entre los que se encuentran están, el Financiero (está relacionado con áreas de planeación y presupuesto), de contratación (como proceso o bien los procedimientos ligados a este), de información y documentación. Adicionalmente, uno de los atributos de los controles corresponde a que se encuentren documentados en el proceso; pudiendo ser documentados en "*…manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso*".

  Adicionalmente, en relación con el modelo de operación por procesos aprobado actualmente en la entidad, es importante manifestar, que los procesos que hacían parte del modelo de operación por procesos aprobados para vigencias anteriores, fueron considerados como

procedimientos e incluidos en los 6 macro procesos que se establecieron y que hacen parte del modelo actual aprobado en la entidad, eliminando las caracterizaciones de dichos procesos; situación que conlleva a la posible pérdida de conocimiento al interior de la Entidad, toda vez que aspectos como las interacciones entre los procesos se eliminaron y las mismas no se reflejan actualmente en los macroprocesos diseñados.

Por lo anterior, el cumplimiento de la directriz relacionada con que "*para los procedimientos asociados a los procesos, el aseguramiento de los riesgos se hará mediante el establecimiento de puntos de control, en aquellas actividades criticas donde se establezca que hay riesgos para el cumplimiento de las mismas, los cuales no hacen parte del mapa de riesgos institucional*"; **implica que se podrían no estar identificando y valorando la totalidad de los riesgos existentes en los procesos / procedimientos / proyectos que se ejecutan en la entidad conforme a la metodología establecida por la Función Pública**.

Así mismo, como parte de los elementos definidos en el alcance de la Política de Administración de Riesgos de la entidad, se plantea, entre otras lo siguiente:

- "*Para gestionar el riesgo la instancia responsable será: El Consejo de Dirección…*"; sin embargo, al revisar la Resolución 144 del 28/04/2020, "*Por medio de la cual se modifica el Comité de Consejo de Dirección de la Contraloría General de Medellín"*, en el artículo segundo, no se detalla ninguna función relacionada con la gestión de los riesgos por parte del Comité.

Es importante al momento de establecer directrices en relación con las responsabilidades de la gestión de riesgos y el control, tener en cuenta lo establecido en la Política de Administración de Riesgos, para la línea estratégica; así como para la primera, segunda y tercera línea de defensa; adicionalmente, lo planteado en la Resolución 604 del 2020 y la Política del Sistema de Control Interno que hace parte del Manual de Políticas de Operación aprobado en la Entidad.

✓ **Términos y Definiciones:** Conforme a la guía, corresponde a "Aquellos relacionados con la administración del riesgo y con los temas que el manual o guía desarrollen sean relevantes para que todos los funcionarios entiendan su contenido y aplicación"; sin embargo, en la Política aprobada

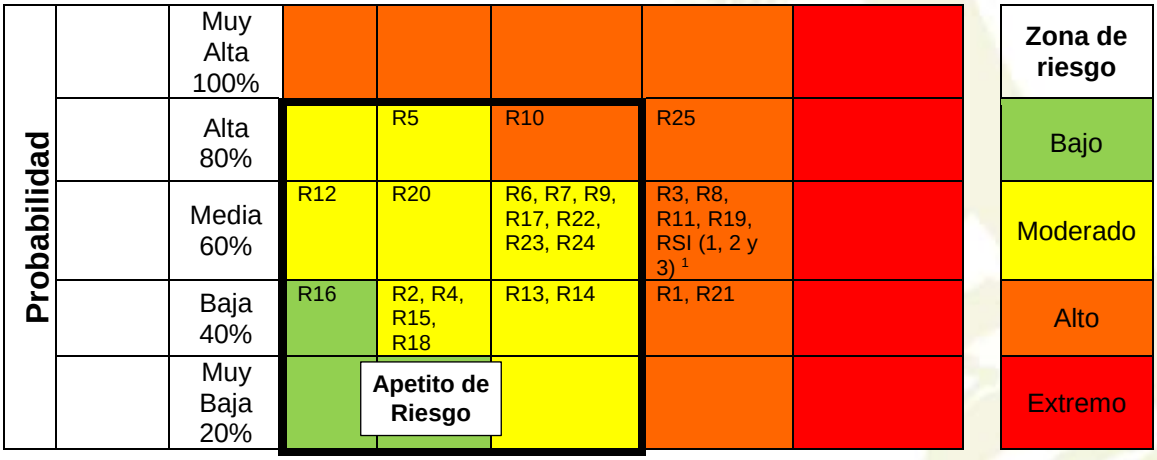
para la entidad, se plantea que "*Los conceptos básicos relacionados con la gestión del riesgo están relacionados en el documento "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas", versión 5 de diciembre de 2020 del Departamento Administrativo de la Función Pública, dispuesto en Isolución en el módulo documentación, listado maestro de documentos externos*"; incumpliendo lo establecido en la guía.

- ✓ **Niveles de aceptación al riesgo:** Conforme a la guía, corresponde a una "*decisión informada de tomar un riesgo particular (NTD GTC 37, Numeral 3.7.1.6). Para riesgos de corrupción es inaceptable*"; al respecto en la Política de administración de riesgos de la entidad, se definió, entre otras, que:

  - *"El apetito de riesgo o nivel de riesgos que la entidad puede aceptar, estará cuando el análisis preliminar del riesgo inherente **se determine entre** la zona de riesgo bajo, con probabilidad muy baja 20% e impacto leve 20%, y la zona de riesgo alta, con probabilidad alta 80% e impacto moderado 60%. (resaltado fuera de texto)*

    Gráficamente la zona relacionada con el apetito al riesgo, conforme a lo aprobado en la Política de Administración del Riesgo, sería como queda a continuación:

Figura 1. Apetito al Riesgo aprobada en la Política de Administración del Riesgo




[1] Los riesgos identificados como RSI (1, 2 y 3), corresponden a los riesgos de Seguridad de la Información identificados para la vigencia 2021.

| | | | | |
|---|---|---|---|---|
| Leve 20% | Menor 40% | Moderado 60% | Mayor 80% | Catastrófico 100% |
| **Impacto** | | | | |

**Fuente:** Matriz Mapa de Riesgos de Gestión V5 2021 al 29/07/2021 y Matriz de Riesgos de Seguridad de la Información al 21/07/2021 – Isolución – Listado Maestro de Registros.

Por lo anterior, conforme a lo establecido en la Política de Administración de Riesgos de la Entidad, de los 28 riesgos identificados (25 de gestión y 3 de Seguridad de la Información), un total de 18 riesgos inherentes, estarían ubicados en el nivel de riesgos que la entidad puede aceptar; siendo importante tener en cuenta que, de éstos, 16 riesgos están en la Zona de Riesgo Moderada y uno (1) en Zona de riesgos Alta.

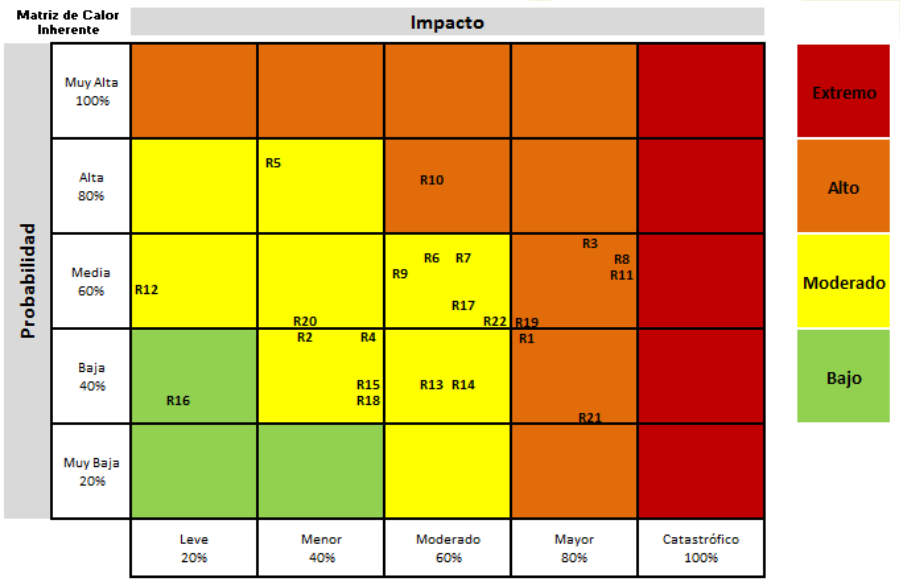
Adicionalmente, se plantea en la Política de la Entidad, que "...*cuándo el análisis del riesgo Inherente este en el mínimo valor posible, no se tendrá que definir controles", sin embargo, al verificar en la matriz de riesgos, se evidenció para el riesgo R16 "Posibilidad de afectación reputacional, por reclamaciones de los servidores públicos por la nómina, debido a la Inconsistencia en la liquidación de la bonificación por servicios prestados en el sistema de nómina",* con una probabilidad *"Baja"* y un impacto *"Leve",* que lo ubica en zona de riesgo *"Bajo",* se tiene definido un control relacionado con que *"Los técnicos operativos quincenalmente, verifican la correcta liquidación de nómina y prestaciones sociales, revisando los resultados vs las novedades y situaciones ingresadas y posteriormente realizan revisión de toda la nómina en forma manual";* lo que estaría en contravía a lo planteado en la Política; siendo importante que en los casos pertinentes, los líderes de los procesos, puedan definir los controles para riesgos que encuentren en dicha zona; lo que implicaría ajustar la Política de Administración de Riesgos.

Frente al tema, la guía de administración de riesgos, establece adicionalmente que*: "**El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar**",* lo que podría implicar, entre otras, que para riesgos relacionados con el cumplimiento normativo en el que su incumplimiento pueda implicar una posible pérdida reputacional o económica para la Entidad, el apetito del riesgo sea cero, es decir que no se acepta ningún riesgo relacionado.

Se evidenció en la Política que se incluye, en relación con el apetito para los riesgos de corrupción, que "*…excepto para los riesgos de corrupción que es inaceptable*"; lo que implica que está conforme con la metodología.

Se verificó la matriz de calor inherente que se tiene anexa a la matriz de riesgos de gestión V5 del 2021 al 15/09/2021, y no se reflejan los riesgos 23, 24 y 25, veamos:

Figura 2. Matriz de calor Inherente




**Fuente:** Matriz Mapa de Riesgos de Gestión al 15/09/2021

Los riesgos 23, 24 y 25 corresponden a los siguientes:

- ✓ Posibilidad de afectación económica y reputacional por la prescripción de los procesos de responsabilidad fiscal, debido a la inactividad procesal; Zona Moderada
- ✓ Posible pérdida reputacional por sanciones y disminución de la certificación anual de gestión de la Contraloría por incumplimiento del Plan Táctico de Auditoría, con la oportunidad y en la cantidad requerida, debido a la falta de recurso humano en la OCI, con las competencias para la ejecución del Plan Táctico de Auditoría y de seguimiento a la ejecución del Plan; Zona Moderada
- ✓ Posible pérdida reputacional y económica por sanciones, procesos disciplinarios y disminución de la certificación anual de gestión de la Contraloría, debido a la inoportunidad en la rendición de la cuenta y que ésta no sea de calidad, consistente, coherente, y veraz; Zona Alta

- *En relación con la tolerancia del riesgo, se plantea que "La tolerancia del riesgo o el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad, será en el nivel alto, con probabilidad mayor 80% e impacto mayor de 80%."; sin embargo, al verificar la escala correspondiente a la probabilidad, no se encuentra la de "mayor 80%".*

✓ **Estructura para la gestión del riesgo:** Conforme a la guía, se deben determinar aspectos como:

- *La metodología a utilizar:* Al verificar en Isolución, no se evidencia la definición de una metodología relacionada con la gestión del riesgo; sin embargo, en la Política de Administración de Riesgos aprobada, se indica como una de las responsabilidades de la Oficina Asesora de Planeación como Segunda Línea de Defensa, es la de "*...definir la metodología para realizar la gestión riesgos en la entidad...*".

- "*En caso de que la entidad haya dispuesto un software o herramienta para su desarrollo, deberá explicarse su manejo*": Al respecto en la Política de Administración de Riesgos, se plantea en relación con el aplicativo Isolución / módulo de riesgos, que: *"...Para el manejo de esta herramienta la Oficina Asesora de Planeación dispondrá en Isolución el manual de usuario del módulo de riesgos...";* sin embargo, al verificar en el módulo de Documentación, en las opciones de Manuales, listado maestro de documentos y listado maestro de registros, no se evidenció ningún documento relacionado con el manual de Usuarios del módulo de riesgos; tampoco se encontró habilitada en el módulo de riesgos, la opción de videoayuda que se tiene en otros módulos; solamente se encontró en el listado maestro de documentos externos, un documento denominado "*Manual Usuarios Módulo Riesgos DAFP*", el cual responde al Manual de Usuario de Isolución para el módulo de riesgos, bajo la guía establecida en la vigencia 2018.

Figura 3. Búsqueda Listado Maestro de Documentos Externos - Isolución


**Fuente:** Isolución, consulta realizada el 07 de julio de 2021

- *"...Incluir la tabla de impactos institucional (ver tabla ilustrativa 3. Niveles para calificar el impacto o consecuencias, p.31);* al verificar en la Política de Administración de Riesgos aprobada en la entidad, en ésta se plantea que: "*Los niveles para calificar el impacto de los riesgos de gestión y de seguridad de la información son los establecidos en el documento "Guía para la administración del riesgo y el diseño de controles en entidades públicas", versión 5 de diciembre de 2020 de la Función Pública*...", sin que se detallen; siendo importante tener en cuenta que en la guía de administración de riesgos se plantea que la tabla propuesta por la Función Pública es ilustrativa y "*Dependiendo del tamaño y complejidad de los procesos en la entidad, la tabla 5 podrá ser ajustada o adaptada a sus necesidades*".

- *"Incluir la periodicidad para el monitoreo y revisión de los riesgos, así como el seguimiento de los riesgos de corrupción";* se pudo evidenciar incluidos en la política en relación con el monitoreo que se *"realizará trimestralmente por parte de la primera línea de defensa";* en el caso de los *"riesgos establecidos en los procesos contractuales estará a cargo del supervisor del contrato, quien dejará evidencia de ello en los informes de supervisión*"; y con respecto a "*los riesgos inherentes al Sistema de Seguridad y Salud en el Trabajo deberán ser monitoreados por el Líder de este Sistema a cargo de la Dirección de Talento Humano";* sin embargo, no se establece en ninguno de los casos en que momento se debe realizar la revisión de los riesgos.

  En relación con el Monitoreo, se establece en la guía que "*le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz...*"; siendo importante tener en cuenta que "*su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los*

*controles establecidos...*"; en este sentido, en el Manual de Políticas de Operación, en la Política del Sistema de Control Interno, se establece para la Segunda Línea de Defensa que se debe realizar el "Monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad"; y en ésta se establece que su rol principal es "*Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa"*

Adicionalmente, se plantea para los riesgos relacionados con los procesos contractuales, que "*la Secretaria General consolidará estos resultados y la posible materialización de algún riesgo, de lo cual presentará informe ante el Consejo de Dirección*", de los demás riesgos, no se dan lineamientos frente a las posibles materializaciones por falta de efectividad en los controles y las gestiones a realizar. Al respecto la guía establece, entre otras, que: "*se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología*"; entendido que el "***evento es un riesgo materializado***"

- *"Incluir los aspectos relevantes sobre los factores de riesgo estratégicos para la entidad, a partir de los cuales todos los procesos podrán iniciar con los análisis para el establecimiento del contexto";* al verificar en la política de administración de riesgos, sólo se evidencia que se enuncian los factores de riesgo, tales como "*…procesos, talento humano, tecnología, infraestructura y eventos externos…";* sin que se incluyan aspectos relevantes conforme a lo requerido.

En relación con la gestión de riesgos, la Contraloría General de Medellín, actualmente se encuentra certificada bajo la norma ISO 9001:2015 y en ésta se establece que uno de "*los beneficios potenciales para una organización de implementar un sistema de gestión de la calidad basado en esta Norma Internacional*", consiste en "***abordar los riesgos y oportunidades*** *asociadas con su contexto y objetivos*"; así mismo que "*esta Norma Internacional emplea el enfoque a procesos, que incorpora el ciclo Planificar – Hacer – Verificar – Actuar (PHVA) y el* ***pensamiento basado en riesgos***"; sin embargo, al analizar la Política de Administración de Riesgos, no se evidencia que se haga alusión a dicha norma y a los requisitos relacionados frente al tema en dicha norma. (Resaltado fuera de texto).

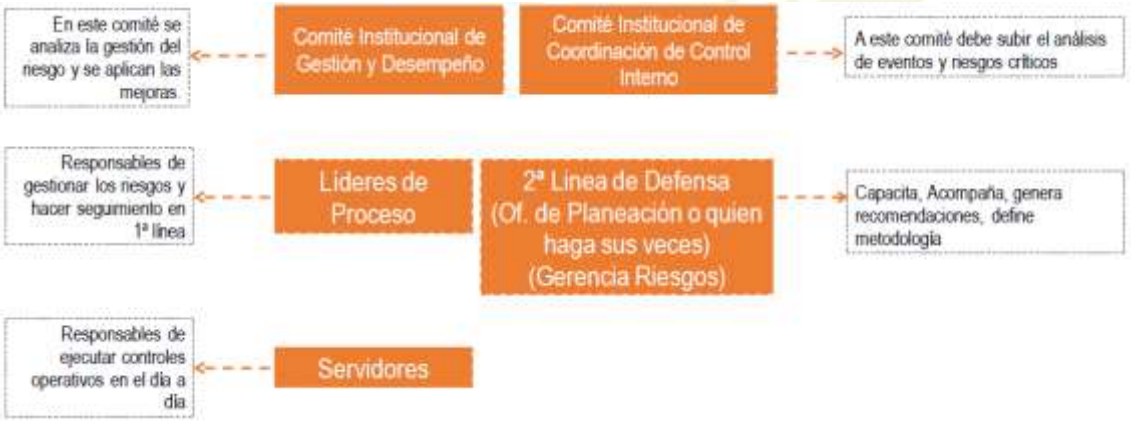
Lo anterior, permite concluir en relación con la Política Institucional de Administración de Riesgos, que no se está dando cumplimiento a la totalidad de

lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas, versión 5; así como que la misma no permite identificar su relación o las gestiones que se adelantan conforme a lo establecido en la norma ISO 9001:2015

## 6.2 INSTITUCIONALIDAD PARA LA ADMINISTRACIÓN DEL RIESGO

La Guía para la Administración del riesgo y el Diseño de Controles en Entidades Pública, versión 5, de diciembre de 2020, plantea que "*El modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017,* en *este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:*"

Figura 4. Operatividad Institucionalidad para la Administración del Riesgo




**Fuente:** Guía para la Administración del riesgo y el Diseño de Controles en Entidades Pública, versión 5, de diciembre de 2020

A continuación se desarrolla lo pertinente con la institucional, entre otras lo relacionado con el Consejo de Dirección, el Comité Institucional de Coordinación de Control Interno – CICCI y las Líneas de Defensa.

## 6.3 COMITÉ DE CONSEJO DE DIRECCIÓN Y COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO - CICCI

De acuerdo a lo anterior, frente a la institucionalidad para la administración de riesgos, se pudo evidenciar, en relación con el **Comité de Consejo de Dirección**, lo siguiente:

- Mediante Resolución 144 del 28/04/2020 se modifica el Comité de Consejo de Dirección de la entidad; sin que se detallen funciones relacionadas con la gestión de riesgos

- Se evidenció la creación del expediente de Mercurio número 18874, en el cual se tienen anexadas las actas de la 1 a la 6; correspondientes a reuniones de los meses de enero, marzo, mayo y junio de 2021 y el expediente número 18019, de la vigencia 2020, con un total de 16 actas.

- Entre las actividades adelantadas en el Comité de Consejo de Dirección, en relación con la gestión de riesgos, se evidencia:

  - ✓ En acta 16 del 22/12/2020, radicado en Mercurio 202190001923 del 22/04/2021, se presenta por parte de la Oficina de Control Interno, el informe de gestión de riesgos con corte a la vigencia 2020.

  - ✓ En acta 01 del 29/01/2021, radicado en Mercurio 202190002293 del 24/05/2021, se plantea que: "*concluyen que la gestión realizada durante el 2020 al Sistema de Gestión de Seguridad y Salud en el Trabajo- SST, si cumplió con la política, los objetivos, el plan de trabajo, el plan de capacitación y* ***el control de riesgos y peligros detectados en la matriz de peligros y riesgos***", resaltado fuera de texto

  - ✓ Adicionalmente se informa por parte de la Jefe de la Oficina Asesora de Planeación, la modificación a diciembre de la metodología para la gestión de riesgos por parte del Departamento Administrativo de la Función Pública y manifiesta que será "*necesario su implementación al interior de la entidad, lo que implica que éstos deberán ser abordados de una manera diferente y por ende tendrán unas causas, unos controles y unos seguimientos distintos*"; se indica que se dará capacitación e invita a todos los directivos "*a involucrarse en este proceso en coordinación con el enlace funcional asignado por cada uno de ellos y así lograr entre todos una construcción de los riesgos más acercada a la realidad de la entidad*"; así mismo se indica que "*la implementación del proceso genera todo un despliegue por parte de la Oficina Asesora de Planeación en cuanto a la asesoría y acompañamiento a todas las áreas y por parte de la Oficina de Control Interno, como tercera*

*línea de defensa, en el cumplimiento de su rol consultor en esta materia, requiriéndose así un apoyo fundamental de todas las dependencias*" y con respecto a los riesgos de corrupción se indica que "*la nueva guía no trae cambios y que de acuerdo con las directrices impartidas el año pasado en el último consejo de Dirección la Oficina Asesora de Planeación había informado que los riesgos no se iban a cerrar y quedaban en stand by hasta tanto no se conocieran las modificaciones a la guía; pero dado que no tuvieron cambios, hace la invitación a aquellas dependencias que tienen a su cargo riesgos de corrupción para adelantar una revisión y actualización y definir si quedarán los mismos, o cuáles se van a quitar porque definitivamente no constituyen un riesgo de corrupción para la entidad*".

- ✓ En acta 02 del 01/03/2021, radicado en Mercurio 202190002295 del 24/05/2021, se informa que se adelantó la capacitación a los servidores de la entidad en la "*…nueva guía de administración del riesgo y frente a cómo se debía iniciar con el levantamiento de la matriz de riesgos de la entidad…*"; indicando que "*...los jefes con sus equipos de trabajo den inicio a la recopilación de la información, pues como primera línea de defensa y responsables de la gestión del riesgo es necesario implementar este trabajo que posteriormente deberán enviar a la Subcontraloría para su consolidación y remisión a la OAP quien se encargará de revisarlos y si es pertinente ajustarlos*"

- ✓ En acta 03 del 01/03/2021, radicado en Mercurio 202190002869 del 30/07/2021, se informa que se "está adelantando el proceso de migración de los riesgos a la nueva metodología de riesgos y diseño de controles, tal como lo establece el DAFP; así mismo, se manifiesta que se están adelantando campañas para la difusión y socialización de la política de administración del riesgo y les recuerda "*que la Oficina Asesora de Planeación estará presta a continuar realizando el acompañamiento respectivo"*

  En relación con el Plan Estratégico de Seguridad Vial – PESV, se indica en la reunión del Consejo, que se "*Durante el mes de marzo se viene trabajando en la actualización del formato para hacer el diagnóstico y caracterización de los riesgos de seguridad vial en la CGM; el cual será remitido a los servidores para diligenciar durante el segundo trimestre de 2021"*

- ✓ En acta 04 del 03/05/2021, radicado en Mercurio 202190002870 del 30/07/2021, se informa por parte de la Jefe de la Oficina Asesora de Planeación, que "*… ya se cuenta en el aplicativo Isolucion con toda la matriz*

*de riesgos actualizado de acuerdo con la nueva versión 5 emitida por el DAFP, lo anterior gracias al trabajo articulado de todos los equipos de trabajo, aclarando que tanto los riesgos de corrupción como los de gestión y seguridad digital quedan abiertos para su consulta";* al respecto, se verificó en Isolución y se evidenció en el módulo de documentación / listado maestro de registros, un archivo en Excel, con el Mapa de Riesgos de Gestión de 2021, versión 5, del 15/09/2021, de los cuales 8 riesgos inherentes están en nivel alto, 16 en nivel moderado y 1 en nivel bajo; a continuación se presenta el consolidado por proceso; veamos:

Tabla 1. Niveles de Riesgo por proceso

| Proceso | Nivel del Riesgo | | | Total general |
|---|---|---|---|---|
| | Alto | Moderado | Bajo | |
| Gestión Estratégica | 2 | 5 | | 7 |
| Control Fiscal | 1 | 2 | | 3 |
| Participación Ciudadana | 1 | | | 1 |
| Gestión del Talento Humano y del Conocimiento | 2 | 3 | 1 | 6 |
| Gestión de Recursos e Infraestructura | 1 | 4 | | 5 |
| Gestión de Evaluación y Seguimiento | 1 | 2 | | 3 |
| **Total general** | **8** | **16** | **1** | **25** |

**Fuente:** Mapa de Riesgos de Gestión de 2021 – Aplicativo Isolución

En relación con los riesgos de corrupción, en el aplicativo Isolución / Modulo de Riesgos, se encuentran registrados los seis (6) riesgos de corrupción para la vigencia 2021; los cuales corresponden a los siguientes:

Tabla 2. Niveles definidos para los Riesgos de Corrupción

| Num | Proceso | Nombre Riesgo | Nivel |
|---|---|---|---|
| CF-16 | Control Fiscal | Posibilidad de presentarse una gestión inadecuada en la realización de las auditorias fiscales, en beneficio propio o de un tercero. | Extremo |
| CF-17 | Control Fiscal | Posibilidad de Fallos de Responsabilidad Fiscal contrarios a derecho para favorecer o perjudicar a tercero | Extremo |
| ES-8 | Gestión de Evaluación y Seguimiento | Posibilidad de Presentar informes o resultados de auditoría que no corresponden a la realidad de la entidad, para beneficio propio o de un tercero | Alto |
| GE-15 | Gestión Estratégica | Posibilidad de omisión en la respuesta de las demandas en beneficio propio o de terceros | Alto |

| | | | |
|---|---|---|---|
| GRI-23 | Gestión de Recursos e Infraestructura | Posibilidad de realizar pagos sin el lleno de los requisitos en beneficio propio o de un tercero | Alto |
| GRI-24 | Gestión de Recursos e Infraestructura | Posibilidad de interés indebido en la celebración de contratos en beneficio propio o de terceros, por el direccionamiento de los estudios previos para seleccionar un determinado contratista que genera multas , sanciones disciplinarias y penales | Alto |

**Fuente:** Mapa de Riesgos de Corrupción de 2021 – Aplicativo Isolución / Módulo de Riesgos

Con respecto a los riesgos relacionados con Seguridad de la Información, se verificó en Isolución y se evidenció en el módulo de documentación / listado maestro de registros, un archivo en Excel, con el respectivo Mapa de Riesgos del 15/09/2021; los cuales están relacionados con el proceso de Gestión de Recursos e Infraestructura y corresponden a los siguientes riesgos:

Tabla 3. Riesgos de Seguridad de la Información definidos en la Entidad

| Riesgo | Activo | Descripción del Riesgo |
|---|---|---|
| Pérdida de la Confidencialidad | Sistemas de Información | La asignación errada de los derechos de acceso y la Gestión deficiente de las contraseñas por parte de los usuarios, lo cual causaría la pérdida de la confidencialidad de los sistemas de información |
| Pérdida de Integridad | Sistemas de Información | Asignación deficiente de permisos y perfiles de usuarios, generan la pérdida de integridad en los sistemas de información. |
| Pérdida de Disponibilidad | Software Hardware | Mantenimiento insuficiente del software y hardware, la pérdida de conexión de internet genera la pérdida de disponibilidad del software, hardware y red. |

**Fuente:** Mapa de Riesgos de Seguridad de la Información de 2021 – Aplicativo Isolución

Adicionalmente, en dicha acta, se plantea que se deberá "*dar inicio con el seguimiento de las acciones para abordar los mismos, las cuales son revisadas de manera permanente, ya que en los seguimientos que se realizan al plan de acción de manera trimestral, se deben aportar en Isolución, los soportes y evidencias que den cuenta del seguimiento que han adelantado para evitar que los riesgos allí contemplados y asociados a cada área se materialicen";* evidenciándose en el módulo de mejora del aplicativo Isolución, el seguimiento a las acciones para abordar los riesgos registradas; así mismo, en el seguimiento que se realiza periódicamente al Plan de Acción Institucional, en la actividad denominada "*Realizar trimestralmente el monitoreo y revisión de los riesgos y actividades de control, acorde con las responsabilidades descritas en la política de administración de riesgos en el*

*rol de primera línea de defensa*" se indica el % de avance o de cumplimiento, se realiza un análisis del resultado y se indica el registro o evidencia al avance reportado.

- ✓ En Acta 05 del 27/05/2021, radicada en Mercurio con el número 202190002871 del 30/07/2021, se informa por parte del Director encargado de la Dirección de Desarrollo Tecnológico, que: "*se adelantan tres seguimientos a los riesgos con el fin de mitigarlos, los cuales son reportados en el aplicativo Isolución"*

- ✓ En acta 06 del 29/06/2021, radicado en Mercurio con el número 202190002872 del 30/07/2021, se solicita que una vez se finalice la evaluación a la gestión de riesgos por parte de la Oficina de Control Interno, en la cual se evalúa la eficacia de las acciones tomadas para abordar los riesgos, sea presentada a dicho Comité.

- ✓ Adicionalmente, se realiza la socialización y aprobación de la Política frente al Sistema de Control Interno, la cual "*fue actualizada conforme al manual operativo de MIPG expedido por el Departamento Administrativo de la Función Pública el pasado mes de marzo de 2021, en lo referente a la Dimensión 7 - MECI, que* ***define las responsabilidades que se deben cumplir bajo el Esquema de Líneas de Defensas, como son: Línea Estratégica Primera línea de Defensa, Segunda Línea de Defensa a cargo de la Oficina Asesora de Planeación y los líderes de los Sistemas de Gestión y algunas áreas puntuales como son el comité de contratación, la Dirección de Recursos Físicos y Financieros y Desarrollo Tecnológico con el tema de Gobierno Digital, y la oficina de Control Interno en la Tercera línea de defensa****". (resaltado fuera de texto);* la cual se encuentra publicada en el aplicativo Isolución / módulo documentación / Manuales en el Manual de Políticas de Operación, código M-GE-PL-002, versión 7

En relación con el Comité Institucional de Coordinación de Control Interno – CICCI, se evidenció lo siguiente:

- Mediante Resolución 604 del 16/12/2020, se actualiza y ajusta la regulación, funcionamiento y composición del Comité Institucional de Coordinación de Control Interno (CICCI) y se subsumen las sesiones ordinarias dentro del Comité del Consejo de Dirección; estableciéndose en relación con la gestión de riesgos, en el artículo 4, literal 8, que se debe "*someter a aprobación del representante*

*legal de la Contraloría General de Medellín la política de administración del riesgo previamente estructurada por parte de la Oficina Asesora de Planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta*"

- Entre las actividades adelantadas en el Comité Institucional de Coordinación de Control Interno, en relación con la gestión de riesgos, se evidencia:

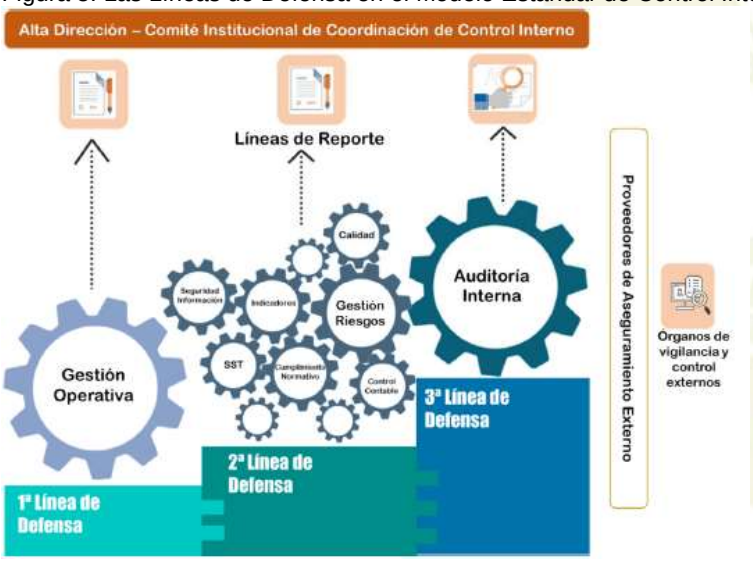
  - ✓ En acta 02 del 01/03/2021, radicado en Mercurio 202190002295 del 24/05/2021, se evidencia la aprobación de la Política de Administración del riesgo; la cual fue "*formulada y elaborada por la oficina Asesora de Planeación de cara a la nueva guía Versión 5, publicada por el Departamento Administrativo de la Función Pública en el mes de diciembre*"; siendo importante tener en cuenta que la Política de Administración de Riesgos, se encuentra publicada en Isolución / módulo documentación / Manuales, como parte del Manual de Políticas de Operación, Código: M-GE-PL-002, Versión 7, la cual fue incluida según el control de cambios el 04/03/2021

  - ✓ En Acta 05 del 27/05/2021, radicada en Mercurio con el número 202190002871 del 30/07/2021, se manifiesta por parte del Jefe de la Oficina de Control Interno, que el Comité Institucional de Coordinación de Control Interno, es "*la instancia donde se realiza el seguimiento de la administración de todos los riesgos de la organización y sus correspondientes controles"* e igualmente se manifiesta en relación con el alcance de los procesos definidos en el Sistema Integrado de Gestión, que *"el alcance de los procesos dada la magnitud que hoy tienen, cobijan actividades que pueden distar de su objeto, de su naturaleza, de su responsabilidad, inclusive de su riesgo, notando dificultad en su administración.*

## 6.4 LÍNEAS DE DEFENSA EN EL MODELO ESTÁNDAR DE CONTROL INTERNO

Complementario a lo anterior, se definen las Líneas de Defensa en el Modelo Estándar de Control Interno; el cual corresponde a "*un esquema de asignación de responsabilidades y roles para la gestión del riesgo y el control, el cual se distribuye en diversos servidores de la entidad, no siendo ésta una tarea exclusiva de las oficinas de control interno. A continuación se muestra gráficamente su funcionamiento y articulación:"*

Figura 5. Las Líneas de Defensa en el Modelo Estándar de Control Interno




**Fuente:** Guía para la Administración del riesgo y el Diseño de Controles en Entidades Pública, versión 5, de diciembre de 2020

En relación con el funcionamiento de las líneas de defensa, tal como se planteó anteriormente, en acta 06 del 29/06/2021, se realiza la socialización y aprobación de la Política frente al Sistema de Control Interno, y en esta se ***"define las responsabilidades que se deben cumplir bajo el Esquema de Líneas de Defensas, como son: Línea Estratégica Primera línea de Defensa, Segunda Línea de Defensa a cargo de la Oficina Asesora de Planeación y los líderes de los Sistemas de Gestión y algunas áreas puntuales como son el comité de contratación, la Dirección de Recursos Físicos y Financieros y Desarrollo Tecnológico con el tema de Gobierno Digital, y la oficina de Control Interno en la Tercera línea de defensa****". (Resaltado fuera de texto)*

### 6.4.1 Línea Estratégica

**Entre las responsabilidades asignadas a la Línea Estratégica** relacionadas con la gestión del riesgo, conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno; en la Política de frente al Sistema de Control Interno, se encuentran las siguientes:

- "*Definición y evaluación de la Política de Administración del Riesgo…*"; siendo evidenciada su definición y aprobación en acta 02 del 01/03/2021 del Comité

Institucional de Coordinación de Control Interno; así mismo se tiene evidencia de su evaluación en acta 16 del 22/12/2020 del Comité de Consejo de Dirección.

- "*Realizar seguimiento y **análisis periódico a la efectividad de los controles**", "Monitoreo permanentemente los riesgos de corrupción*" y "***Monitoreo al estado de los riesgos aceptados (apetito por el riesgo**), con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad";* en la revisión realizada a las actas del Comité del Consejo de Dirección y al Comité Institucional de Coordinación de Control Interno, no se evidenció el cumplimiento de estas actividades de manera periódica, conforme a lo requerido.

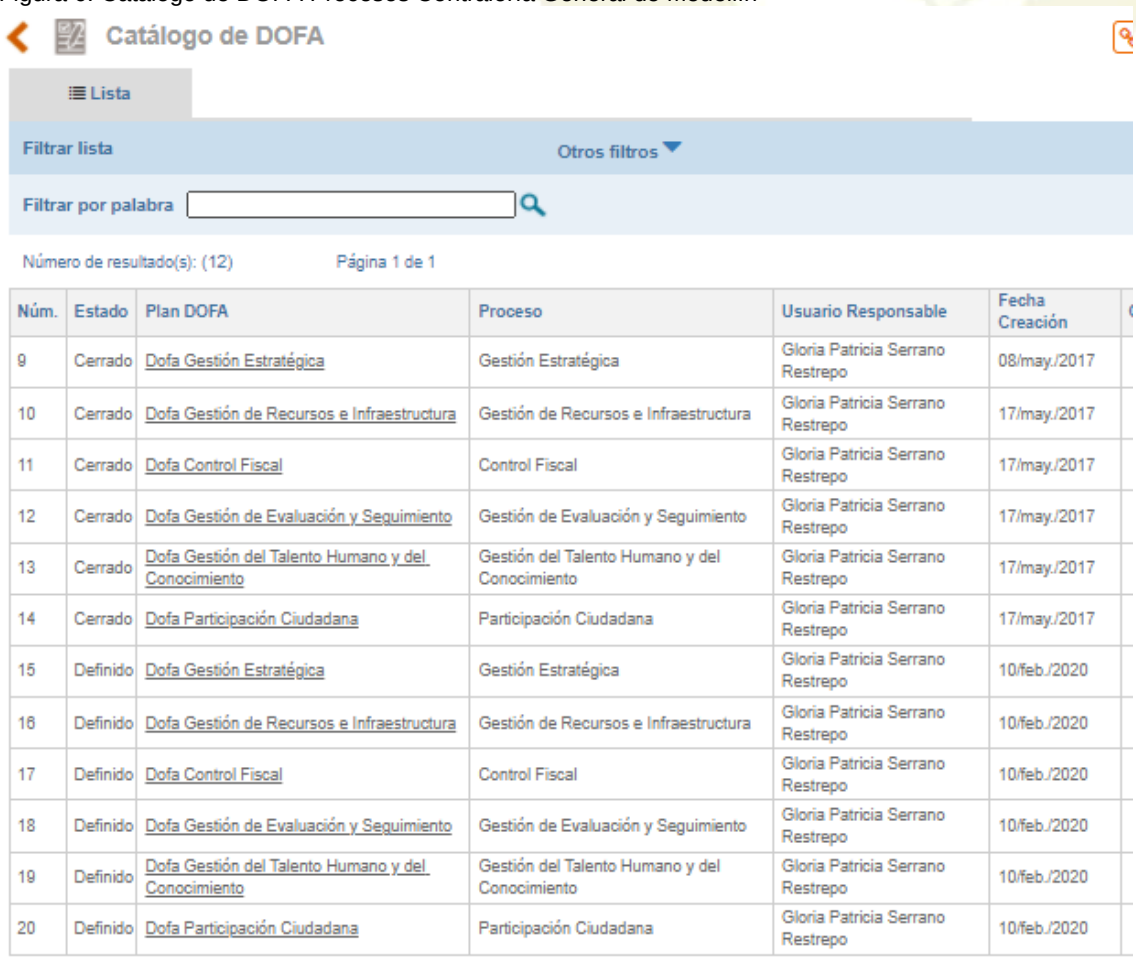
### 6.4.2 Primera Línea de Defensa

Para la **Primera Línea de Defensa**, se definen en el Manual de Políticas de Operación, entre otras, las siguientes responsabilidades:

- *"La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos*"; siendo evidenciada la realización de estas actividades, entre otras, por la socialización de los mapas de riesgos realizada en Comité de Consejo de Dirección, acta 04 del 03/05/2021; así como el seguimiento que se realiza periódicamente en el aplicativo Isolución / Modulo de Mejora a las acciones para abordar los riesgos establecidas.

- *"Revisión de las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico");* sin embargo, en las reuniones realizadas con los diferentes líderes de procesos se pudo evidenciar que durante la vigencia 2021, no se había realizado una revisión del contexto estratégico previo a la revisión y actualización de los riesgos relacionados con los procesos que se lideran y al verificar en el aplicativo Isolución / módulo de riesgos / contexto estratégico, se evidencia el contexto para los 6 procesos con fecha de creación del 08/05/2017 y posteriormente del 10/02/2020; veamos:

Figura 6. Catálogo de DOFA Procesos Contraloría General de Medellín



Catálogo de DOFA

Lista

Filtrar lista Otros filtros

Filtrar por palabra

Número de resultado(s): (12) Página 1 de 1

| Núm. | Estado | Plan DOFA | Proceso | Usuario Responsable | Fecha Creación |
|---|---|---|---|---|---|
| 9 | Cerrado | Dofa Gestión Estratégica | Gestión Estratégica | Gloria Patricia Serrano Restrepo | 08/may./2017 |
| 10 | Cerrado | Dofa Gestión de Recursos e Infraestructura | Gestión de Recursos e Infraestructura | Gloria Patricia Serrano Restrepo | 17/may./2017 |
| 11 | Cerrado | Dofa Control Fiscal | Control Fiscal | Gloria Patricia Serrano Restrepo | 17/may./2017 |
| 12 | Cerrado | Dofa Gestión de Evaluación y Seguimiento | Gestión de Evaluación y Seguimiento | Gloria Patricia Serrano Restrepo | 17/may./2017 |
| 13 | Cerrado | Dofa Gestión del Talento Humano y del Conocimiento | Gestión del Talento Humano y del Conocimiento | Gloria Patricia Serrano Restrepo | 17/may./2017 |
| 14 | Cerrado | Dofa Participación Ciudadana | Participación Ciudadana | Gloria Patricia Serrano Restrepo | 17/may./2017 |
| 15 | Definido | Dofa Gestión Estratégica | Gestión Estratégica | Gloria Patricia Serrano Restrepo | 10/feb./2020 |
| 16 | Definido | Dofa Gestión de Recursos e Infraestructura | Gestión de Recursos e Infraestructura | Gloria Patricia Serrano Restrepo | 10/feb./2020 |
| 17 | Definido | Dofa Control Fiscal | Control Fiscal | Gloria Patricia Serrano Restrepo | 10/feb./2020 |
| 18 | Definido | Dofa Gestión de Evaluación y Seguimiento | Gestión de Evaluación y Seguimiento | Gloria Patricia Serrano Restrepo | 10/feb./2020 |
| 19 | Definido | Dofa Gestión del Talento Humano y del Conocimiento | Gestión del Talento Humano y del Conocimiento | Gloria Patricia Serrano Restrepo | 10/feb./2020 |
| 20 | Definido | Dofa Participación Ciudadana | Participación Ciudadana | Gloria Patricia Serrano Restrepo | 10/feb./2020 |

**Fuente:** Aplicativo Isolución / Modulo Riesgos / Contexto Estratégico, consulta realizada el 21Oct2021

- En el Manual de Políticas de Operación se incluyen responsabilidades para **la Primera Línea de Defensa** que no son claras en su redacción, que consideramos hacen referencia a una autoevaluación y que corresponden a las siguientes:

  - ✓ *"**Verificación**, en el marco de la política de riesgos institucional, **que la identificación y valoración del riesgo de la primera línea sea adecuada** frente al logro de objetivos y metas.*
  - ✓ ***Verificación de que el diseño del control establecido por la primera línea de defensa sea pertinente** frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito,*

*periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y* ***efectuar las recomendaciones*** *a que haya lugar ante las instancias correspondientes* ***(primera****, segunda, y línea estratégica)". Resaltado fuera de texto;* para lo cual, uno de los elementos que se deben valorar por parte de los líderes al momento de definir los controles y que queda plasmado en el mapa de riesgos, es si cumplen atributos como el tipo, si es manual o automático, la frecuencia, si está o no documentado y la evidencia; sin embargo, no es posible evidenciar el análisis sobre la adecuada segregación y el tratamiento en caso de desviaciones.

### 6.4.3 Segunda Línea de Defensa

Respecto a **la Segunda Línea de Defensa**, entre quienes se incluyen conforme a la Política frente al Sistema de Control Interno, "…***la Oficina Asesora de Planeación y los líderes de los Sistemas de Gestión y algunas áreas puntuales como son el comité de contratación, la Dirección de Recursos Físicos y Financieros y Desarrollo Tecnológico con el tema de Gobierno Digital…";*** a continuación se presenta el análisis realizado para las gestiones adelantadas por la Oficina Asesora de Planeación y algunos de los Comités; veamos:

En relación con la Oficina Asesora de Planeación; en cumplimiento de sus responsabilidades se evidenció, entre otras, para las responsabilidades que se detallan a continuación, lo siguiente:

- La Resolución 604 de 2021, establece que la Oficina Asesora de Planeación como Segunda Línea de Defensa, debe estructurar la Política de administración de riesgos para que posteriormente sea sometida a aprobación del representante legal de la Contraloría General de Medellín; de lo cual se pudo evidenciar su cumplimiento, toda vez que como se manifiesta en el memorando 202100003818 del 20/05/2021, "*se realizó actualización de la Política de Administración del Riesgo, la cual fue presentada ante el Comité CICCI, la misma que fue aprobada por éste, tal como consta en el acta No.01 de 2021 CICCI – Acta No. 2 del Consejo de Dirección*"; adicional a lo anterior, se realizaron campañas de sensibilización y para su apropiación, mediante la generación de varias actividades y un despliegue interno.

- *En el Manual de Políticas frente al Sistema de Control Interno, se establece la de "Acompañar, orientar y diseñar herramientas dirigida a los líderes de procesos, para facilitar la identificación, diseño e implementación de controles*

*que permitan reducir, mitigar y/o eliminar los riesgos.";* evidenciándose en cumplimiento de esta responsabilidad, lo siguiente, entre otras que mediante memorando 202100001770 del 25/02/2021, se solicita dar inicio con la construcción, identificación de los riesgos y plasmarlos en la matriz de riesgos; teniendo en cuenta que se había impartido capacitación previamente sobre la nueva guía a todos los directivos y sus enlaces; en este se recomienda que se haga en mesas de trabajo o grupos primarios y de requerirse contar con el acompañamiento por parte de la Oficina Asesora de Planeación. Se anexa la Matriz Mapa de Riesgos, la Guía de Administración de Riesgos y Diseño de Controles Entidades Públicas, versión 5 de 2020 de la Función Pública y presentación en Power Point con memorias de Capacitación del DAFP

- Adicional a la anterior, se establece la de "*Asesorar, sobre el diseño de los controles y realizar la evaluación a los mismos";* conforme a lo informado mediante memorando 202100003818 del 20/05/2021, *"se realizaron reuniones y mesas de trabajo de asesoría y acompañamiento virtuales con los líderes de procesos y sus equipos de trabajo, para la revisión y validación de los riesgos, previo ejercicio interno realizado con cada dependencia";* así mismo que *"se hicieron mesas de trabajo de acompañamiento con la Dirección de Desarrollo Tecnológico, para la revisión de los riesgos de Seguridad Digital y la identificación y actualización de los mismos";* lo cual se pudo evidenciar en los documentos que se anexan como soporte de lo informado.

- Igualmente se establece que se debe realizar "*revisión de las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico)*" y conforme al memorando 202100003818 del 20/05/2021, se plantea que:

  "*Es importante tener en cuenta que existe una Política de Administración del Riesgo en la cual se establece;*
  *En la contratación de la entidad, los riesgos asociados serán gestionados con base en la guía que para ello establezca Colombia Compra Eficiente o aquella que la modifique; así mismo los riesgos de seguridad y salud en el trabajo se trabajarán acorde con lo que establezca la normativa definida para tal fin, y ambos riesgos tampoco harán parte del mapa de riesgos institucional.*
  *De conformidad con lo anterior, los riesgos de contratación son revisados por Secretaria General y los riesgos consultados no hacen parte del Mapa de riesgos institucional general y por consiguiente tampoco hacen parte del contexto estratégico*"

Lo planteado anteriormente, no permite concluir que efectivamente se haya realizado el monitoreo del contexto estratégico y la revisión de la exposición al riesgo con los grupos de valor diferente a los empleados, quienes efectivamente participaron de la revisión de los mapas de riesgos, conforme a lo evidenciado anteriormente.

Respecto al tema, la norma ISO 9001:2015, en el numeral 4.1 Comprensión de la Organización y de su contexto", la organización "*debe determinar las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica, y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la calidad*. Así mismo que "*la organización debe realizar el seguimiento y la revisión de la información sobre estas cuestiones externas e internas*"; considerando que estás cuestiones pueden incluir "*factores positivos y negativos o condiciones para su consideración"* y que la "*comprensión del contexto externo puede verse facilitada al considerar cuestiones que surgen de los entornos legal, tecnológico, competitivo, de mercado, cultural, social y económico, ya sea internacional, nacional, regional o local*" y en relación con el contexto interno "*puede verse facilitada al considerar cuestiones relativas a los valores, la cultura, los conocimientos y el desempeño de la organización*".

Adicionalmente, tal como se manifestó anteriormente, en las reuniones realizadas con los líderes de los procesos, así como en el aplicativo Isolución / módulo de riesgos y en el archivo en Excel que se remitió para la identificación, análisis y valoración de los riesgos, no se evidencia revisión del contexto estratégico previo a la aplicación de la metodología en 2021 y que fuera actualizada a Diciembre de 2020 por parte de la Función Pública.

- En la Política de Administración de Riesgos, se establece, entre otras, para la Oficina Asesora de Planeación, como Segunda Línea de Defensa, en relación con la responsabilidad que debe *"Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende, generando las alertas cuando a ello haya lugar"* y *"Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo, a través del acompañamiento"* y conforme al memorando 202100003818 del 20/05/2021, se informa que *"para asegurar que los controles se hagan por parte de la primera línea de defensa, éste se hace a través del seguimiento (con recomendaciones), asesorías, revisión, acompañamiento en la identificación y valoración de los*

*riesgos, y socialización en el Consejo de Dirección con recomendaciones puntuales mediante un informe ejecutivo presentado a la Alta dirección; validando que los controles sean los adecuados para minimizar las causas identificadas y verificando que los controles si estén siendo aplicados y revisados en caso de materialización. (Ver anexo 9 Presentación a partir de la diapositiva 15, anexa al Acta No. 03 del Consejo de Dirección";* al revisar la presentación realizada en Consejo de Dirección, se evidenció que se informó que *"en el primer trimestre 2021, se tramitó una (1) PQRSD con respuesta extemporánea, incumplimiento que no fue cargado a ninguna dependencia, toda vez, que al revisar el error proviene desde taquilla en la ruta donde fue cargada la misma; no obstante, al ser la C.A de PC el área donde se encuentra identificado este riesgo deben diligenciar el formato de control de salidas no conformes, revisar causas y controles, y elaborar plan de acción en el módulo de riesgos; además* ***este evento deben llevarlo ante el CICCI";*** sin embargo, no se evidencia algún pronunciamiento en relación con el diseño de los controles y que estos funcionen como se pretende, conforme a la política definida; adicionalmente, no se evidencia que se haya presentado en el CICCI lo relacionado con el riesgo de gestión de las PQRSD de acuerdo a lo planteado en el acta de Consejo de Dirección.

En relación con el seguimiento al Plan de Acción Institucional 2021, en los informes que se realizan trimestralmente por parte de la Oficina Asesora de Planeación, a la actividad *"Realizar trimestralmente el monitoreo y revisión de los riesgos y actividades de control, acorde con las responsabilidades descritas en la política de administración de riesgos en el rol de primera línea de defensa";* se informa que: *"Las áreas vienen cumpliendo con los monitoreos, ver seguimientos individuales" y para la actividad ".*

Lo anterior, permite evidenciar que la Oficina Asesora de Planeación ha venido cumpliendo con las responsabilidades asignadas como Segunda Línea de Defensa; siendo importante fortalecer la presentación de informes en el Comité Institucional de Coordinación de Control Interno, en relación con el monitoreo del contexto estratégico, la evaluación del diseño de los controles, su efectividad y que funcionen como se requiere, generando las alertas tempranas requeridas por la entidad; así mismo, evaluar e informar sobre el cumplimiento de la Política de Administración del Riesgo.

En relación con las gestiones adelantadas por los diferentes Comités en la Entidad, exceptuando el Comité de Consejo de Dirección y el Comité Institucional de Coordinación de Control Interno - CICCI, se procedió a verificar en las Resoluciones

que reglamentan para algunos de los Comités sus funciones, si existía o no una función relacionada con la gestión de riesgos en específico, conforme a lo establecido en el Manual de Políticas de Operación; evidenciando lo siguiente:

- En la Resolución número 483 del 17/11/2020, "*por medio del cual se modifica el Comité Interno de Archivo*"; se establece en el artículo 3. Funciones, numeral 7. "*aprobar el plan de aseguramiento documental con miras a proteger los documentos contra diferentes riesgos*"; sin que se establezcan funciones adicionales relacionadas con la gestión de riesgos.

- La Resolución número 232 del 08/07/2020, "*por medio de la cual se actualizan y ajustan las disposiciones atinentes a la composición, regulación y funcionamiento del Comité de Conciliación y Defensa Judicial de la Contraloría General de Medellín y se dicta el Reglamento Interno*", establece en el *artículo 24. POLÍTICA DE PREVENCIÓN DEL DAÑO ANTIJURÍDICO*, establece en el *Parágrafo 1. Que "en la eventualidad que en la Contraloría General de Medellín no se presenten los daños antijurídicos mencionados en precedencia,* ***la política de prevención del daño antijurídico deberá construirse con el fin de mitigar los riesgos*** *existentes que puedan presentarse al interior de la entidad y que generen posibles acciones judiciales en su contra*" (resaltado fuera de texto); sin embargo no se establecen elementos adicionales en relación con la gestión de riesgos.

- En la Resolución 357 del 25/05/2021, "*por medio de la cual se actualiza el Comité Técnico de Auditorías Fiscales de la Contraloría General de Medellín*", se establece en el *artículo 3. Funciones del Comité Técnico*, el "*aprobar la matriz de riesgo fiscal*", requerida para la planificación del proceso de Control Fiscal, más no con la ejecución propiamente dicha del proceso y "*rendir un informe mensual de las actividades de control a los riesgos del proceso auditor*"; sin embargo no se establecen funciones relacionadas con la identificación, análisis y valoración de los riesgos propios del proceso de Control Fiscal.

- La Resolución 261 del 19/04/2021, "*por medio de la cual se crea y reglamenta el Comité de Revisión de Auditorías- CRA en la Contraloría General de Medellín*", no estable funciones en relación con la gestión de riesgos para dicho Comité.

- En el Proceso de Participación Ciudadana; no se cuenta con Comités

- El Comité de Compras e Inventarios de la Contraloría General de Medellín, Resolución 06 del 04/01/2017; modificada por la Resolución 049 del 28/03/2019; en dichas resoluciones no se establecen funciones relacionadas con la identificación, análisis y valoración de los riesgos.

- En la Resolución número 618 del 21/12/2020, "*Por medio de la cual se actualiza el Comité Técnico de Inventarios (COTEIN) en la Contraloría General de Medellí*n", en el *artículo 3: Funciones del Comité*, se establece en el literal e) que debe "*Identificar los riesgos inherentes a cada una de las actividades del proceso contable, así como los respectivos controles que deben implementarse para cada uno de los riesgos identificados*"

- En la Resolución 620 del 21/12/2020, "por medio de la cual se actualiza el Comité Financiero de la Contraloría General de Medellín", no se establecen funciones relacionadas con la gestión de los riesgos.

- En la Resolución número 390 del 13/10/2020, "*por medio de la cual se actualiza la conformación y funciones del Comité de Coordinación del Plan Institucional de Gestión Ambiental PIGA y se reafirma la Política Ambiental de la Contraloría General de Medellín*", no se definen funciones relacionadas con la gestión de riesgos.

- En la Resolución número 308 del 05/05/2021, "*por medio de la cual se actualiza el Programa de Formación y Capacitación de la Contraloría General de Medellí*n", se establecen en el artículo 19 las funciones del Comité de Capacitación y al verificar no se evidencian funciones relacionadas con la gestión de riesgos.

- El Acuerdo 029 del 11/11/2014, "*por medio del cual se establece el Estatuto del Programa de Vivienda de la Contraloría General de Medellín*", establece en el artículo 3, las funciones del Comité del Programa de Vivienda; sin que se establezcan funciones relacionadas con la gestión de riesgos del programa; similar a lo evidencia en la Resolución 010 del 17/01/2017 "*por medio de la cual se reglamente el Programa de Vivienda para los Servidores Públicos de la Contraloría General de Medellín"*.

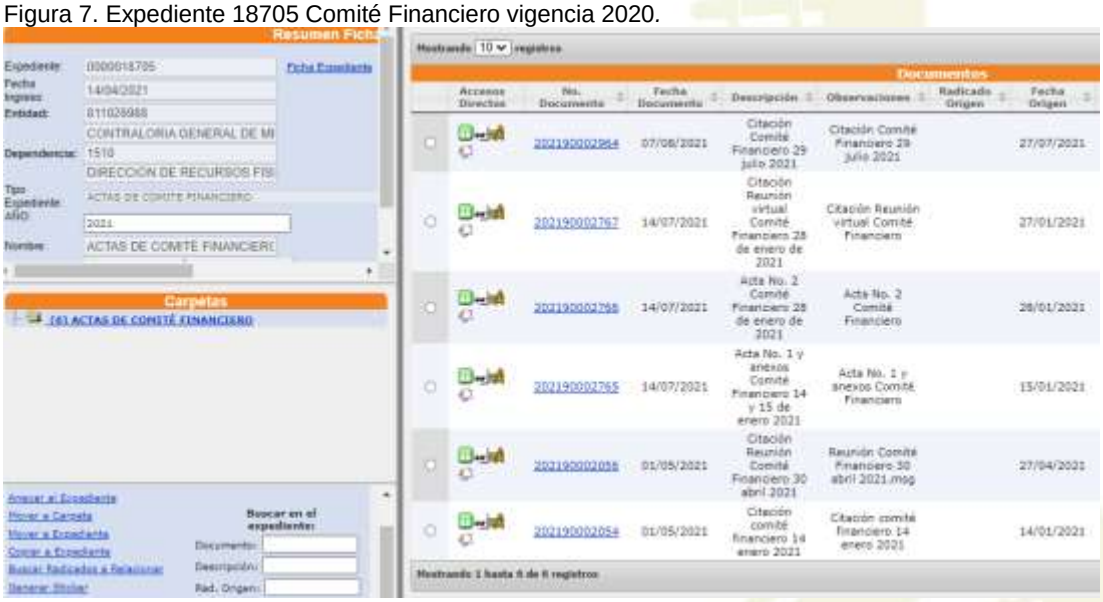
- En la Resolución número 655 del 30/12/2020 "*por medio de la cual se crea el comité de bienestar y motivación, y se adopta el sistema de estímulos en la Contraloría General de Medellín*", no se evidencian funciones relacionadas con la gestión de riesgos.

Lo anterior, permitió evidenciar que para los diferentes Comités analizados, solamente para el *Comité Técnico de Inventarios (COTEIN)*, se estableció entre sus funciones lo relacionado con la gestión de riesgos.

Adicionalmente, en cumplimiento de las responsabilidades establecidas en el Manual de Políticas de Operación, en relación con la gestión de riesgos y como Segunda Línea de Defensa, se procedió a verificar en las actas registradas en Mercurio, para algunos Comités, si se habían tratado específicamente sobre la gestión de riesgos, evidenciándose lo siguiente:

- Para el Comité Financiero, se evidenciaron registradas 2 actas en el expediente de Mercurio número 18705; y entre los temas tratados se encuentran el cierre financiero 2020, la aprobación del presupuesto para la vigencia 2021 y la aprobación de traslado presupuestal; evidenciándose registrado 4 citaciones a reunión y 2 actas; conforme se detalla en la siguiente imagen:

Figura 7. Expediente 18705 Comité Financiero vigencia 2020.




**Fuente:** Aplicativo Mercurio

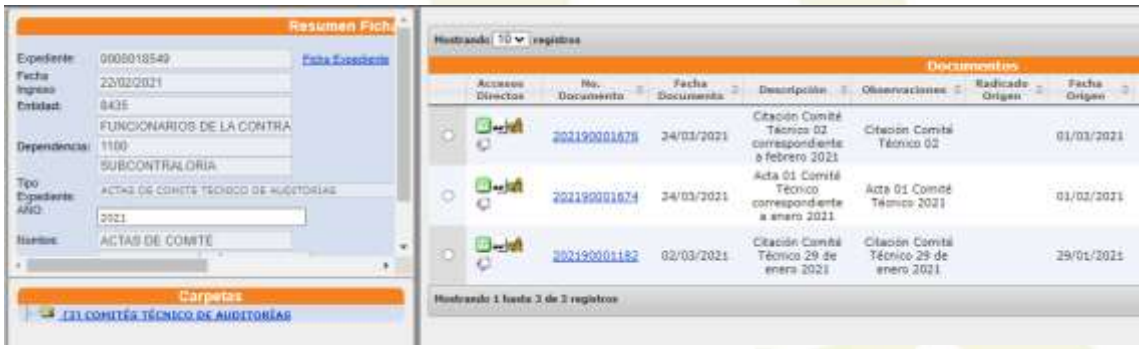
- Para el Comité Técnico de Inventarios se verificó el expediente 18459 y no se encontró información registrada en dicho expediente; tal como se evidencia a continuación:

Figura 8. Expediente 18459 Comité Técnico de Inventarios vigencia 2020.


**Fuente:** Aplicativo Mercurio

- Para el Comité Técnico de Auditorias, se verificó el expediente 18549 y se evidenciaron 2 citaciones y 1 acta registrada en dicho expediente; al analizar el acta se observa, entre otras, que se plantea lo siguiente: "respecto a la actividad de control del riesgo de corrupción denominada "Notificar el hecho a la Subcontralora en caso de divulgación o filtración de información confidencial", se manifiesta por parte de las CAAF, que no se tiene evidencia de que se haya presentado el hecho, por lo tanto no se materializó el riesgo". El expediente contiene los registros que se presentan a continuación:

Figura 9. Expediente 18549 Comité Técnico de Auditorías vigencia 2020.




**Fuente:** Aplicativo Mercurio

En relación con la custodia de la información y de acuerdo a lo evidenciado anteriormente, es importante tener en consideración la conclusión presentada por la Oficina de Control Interno durante la vigencia 2021, en el informe de evaluación independiente "Evaluación y Seguimiento al Cumplimiento de las Funciones Comités CGM"; en la cual se plantea lo siguiente:

*"Como resultado de esta auditoría, se observó que en algunos de los comités evaluados, en lo relacionado con la elaboración, firma, aprobación, archivo, custodia de las actas de los diferentes comités, no se han realizado con el rigor requerido o establecido en las resoluciones. Además este actividad debe ejecutarse y su definición estar alineada a las disposiciones del Manual Sistema Integral de Gestión código M-GE-PL-001 versión 18: "**Los secretarios técnicos de los Comités son los responsable de elaborar el acta y de mantener actualizados los expedientes físicos y electrónicos, por lo cual deben archivar los documentos generados en la carpeta custodiada en la Dependencia que tiene a cargo dicho comité de acuerdo a lo estipulado en la Tabla de Retención Documental…**". (Resaltado fuera de texto)*

Y complementando la revisión realizada durante la presente evaluación, en dicho informe, adicionalmente se plantea lo siguiente en las conclusiones:

*"Verificado el cumplimiento de las funciones de los comités establecidas en las diferentes resoluciones objeto de esta auditoría, se concluye que se debe tener especial cuidado en el cumplimiento de éstas y llevar registro de su desarrollo en las actas de las reuniones. **Se evidenció que algunos comités no estaban dando cumplimiento a sus funciones y/o no estaban dejando evidencia de la ejecución de las mismas**. Las acciones de los comités apoyan a la entidad en el cumplimiento de su misión, además de **generar las alertas oportunas en las dependencias para dar cumplimiento a los objetivos y metas estratégicas definidas por la entidad, y así garantizar la efectividad del Sistema de Control Interno de la Contraloría General de Medellín**.*

*Por otro lado, **los controles que deben ejercer los comités de la entidad, los cuales están inmersos en las funciones o responsabilidades, que se asignaron en la creación de los mismos, son los que garantizan minimizar la materialización de riesgos**. Los controles efectivos nos permiten la optimización de los recursos, una adecuada gestión administrativa, financiera, operativa, además de identificar las acciones a mejorar en los diferentes procesos y procedimientos que se ejecutan en la entidad y que finalmente la impactan a través de la toma de decisiones acertadas y oportunas. Por lo anterior **se debe garantizar, como se ha dicho reiteradamente, el cumplimiento de las funciones que actúan como controles que desarrollan los diferentes comités**". (Resaltada fuera de texto).*

### 6.4.4 Tercera Línea de Defensa

De conformidad con las políticas de operación establecidas en el Manual de Políticas de Operación, se verificó para la Tercera Línea de Defensa, el cumplimiento, entre otras, de las siguientes funciones relacionadas con la gestión de riesgos:

- "*Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo*"; al respecto se evidenció el memorando número 202100007975 del 15/09/202, a través del cual se realiza recomendación con alcance preventivo relacionada con la implementación de la Resolución 1519 de 2020 y los estándares y directrices para publicar la información señalada en la Ley 1712 de 2014; adicionalmente, mediante memorando 202100007597 del 03/09/2021 se remite la Evaluación Parcial Segundo Trimestre 2021 y anual de certificación AGR 2020 y se informa que la Oficina de Control Interno continúa celebrando reuniones con las dependencias para capacitar en la metodología de la evaluación, interpretar resultados y determinar las acciones que permitan a la Contraloría lograr una calificación satisfactoria"; información que es igualmente compartida periódicamente en reunión de Consejo de Dirección, con el fin de que se tomen las acciones pertinentes.

- *"Evaluación de la gestión del riesgo de la entidad de forma integral";* para la vigencia 2020 se realizó esta evaluación y la misma fue socializada en Comité Consejo de Dirección, tal como consta en acta 16 del 22/12/2020.

- En la evaluación realizada, no se evidencia la ejecución de la responsabilidad relacionada con "*Recomendar a los líderes de procesos, sobre controles que permitan reducir, mitigar y/o eliminar los riesgos"; así c*omo la *"**Asesoría proactiva** y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y **sobre las responsabilidades en materia de riesgos"*** (Resaltado fuera de texto)

En relación con la Segunda y Tercera Línea de Defensa, el Manual de Políticas de Operación, establece para la Tercera Línea de Defensa, que debe: "*Asesorar de forma articulada con la Oficina Asesora de Planeación, sobre la identificación y diseño de controles a la primera línea (1 ª) y (2ª) línea de defensa"* y para la Segunda Línea de Defensa, que debe realizar un *"Trabajo coordinado con las Oficina de Control Interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno";* sin embargo no se tiene evidencia del cumplimiento de estas

responsabilidades compartidas por parte de la Segunda y Tercera Línea; siendo importante tener en cuenta, que entre las recomendaciones que se han hecho de manera explícita durante los informes de evaluación a la gestión de riesgos y que han sido presentados en Consejo de Dirección, está el hecho de que se trabaje de manera articulada entre las Oficinas de Control Interno y la Oficina Asesora de Planeación, con el fin de que se consolide la gestión de riesgos al interior de la entidad.

Lo anterior permite evidenciar la importancia de fortalecer en la entidad la gestión que se debe realizar en las diferentes líneas de defensa establecidas y de esta forma consolidar la gestión de riesgos al interior de la entidad.

# 7. APLICACIÓN DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS EN LA CGM

## 7.1 RIESGO DE GESTIÓN

De acuerdo con la metodología establecida por la Función Pública, para la identificación del riesgo, se deben aplicar las siguientes fases:

- Análisis de objetivos estratégicos y de los procesos
- Identificación de los puntos de riesgo
- Identificación de áreas de impacto
- Identificación de áreas de factores de riesgo
- Descripción del riesgo
- Clasificación del riesgo

Por lo anterior, se procede a analizar cada una de las fases; siendo importante tener en cuenta que el análisis que se realiza corresponde a los riesgos de gestión; toda vez que la metodología presenta en los numerales 4 y 5, los lineamientos relacionados con posibles actos de corrupción y de seguridad de la información respectivamente; sin embargo, existen elementos que son comunes a los diferentes tipos de riesgos.

### 7.1.1 Análisis de Objetivos Estratégicos y de los Procesos

Para verificar el cumplimiento de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 5, de la Función Pública, se verificó en el aplicativo Isolución / Modulo Documentación / Listado Maestro de Registros, el documento denominado "*Contexto Estratégico de la CGM*" y para el caso específico del compromiso adquirido por parte de la Sra. Contralora en el Concejo de Medellín, se procedió a validar lo pertinente a la Evaluación de las Políticas Públicas; evidenciándose lo siguiente:

- Se evidencia incluida en la misión, al plantear que se hará "*…énfasis en la evaluación de las políticas públicas…*" y en la visión, planteando que: "…será una entidad líder en la implementación de procesos para la evaluación de políticas públicas…"

- No se hace alusión de la evaluación de las políticas públicas en la Política Integral de Gestión de la Entidad.

- Se incluyó en la directriz estratégica relacionada con la "*Vigilancia y Control Fiscal*" y se determinó como uno de los objetivos estratégicos el "*evaluar el desempeño de las políticas públicas determinando su impacto y pertinencia*" y como estrategia asociada FODA, la del "*Fortalecimiento del control fiscal Macro desde la evaluación y seguimiento de las Políticas Públicas…*"; sin embargo al verificar la matriz FODA que se encuentra anexa, no se evidencian definidas fortalezas, amenazas, debilidades y oportunidades específicas; entre otras, lo relacionado con que no se dispone de metodología específica para realizar la evaluación y el seguimiento de las Políticas Públicas y que tal como se plantea en el análisis DOFA realizado, se tiene identificado como amenaza para el ejercicio eficiente y eficaz del control fiscal frente a los sujetos de control, la "Insuficiencia de personal idóneo con los perfiles adecuados y requeridos"; situación que podría impactar en el logro del objetivo estratégico.

- En el análisis DOFA realizado y que conforme a lo verificado se evidenció incluido en el Plan Estratégico Institucional 2020 – 2021 del 21/07/2020, actualizado al 30/09/2021 en el que se evidencian otras fortalezas y debilidades relacionadas con el proceso de Control Fiscal, que podrían impactar sobre el logro del objetivo estratégico relacionado con la evaluación y seguimiento de las Políticas Públicas; entre las que se encuentran las siguientes:

  - ✓ "*Se cuenta con servidores de experiencia en el control fiscal*" (**Fortaleza**)
  - ✓ "Amplia cobertura del control fiscal en el alcance representado en los sujetos de control" (**Fortaleza**)
  - ✓ Los alcances definidos para las Contralorías Auxiliares de Auditoría Fiscal - CAAF no están actualizados a las necesidades del control fiscal y no guardan coherencia con la reestructuración de los sujetos de control (**Debilidad**).
  - ✓ Cambios normativos que afectan el ejercicio del control fiscal (**Amenaza**)**.**

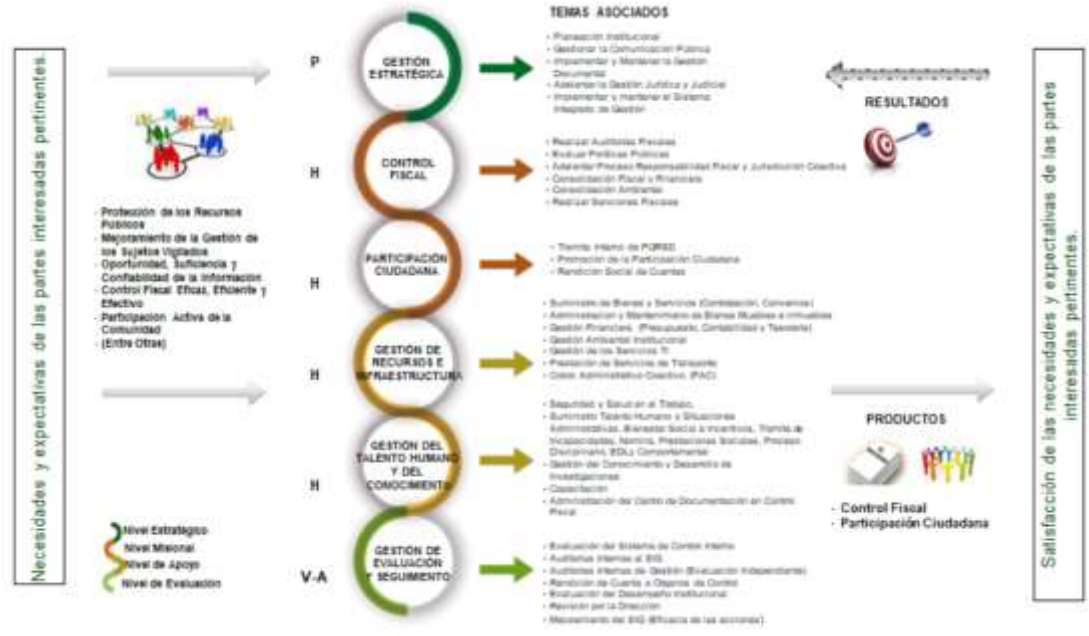
  Es importante tener en cuenta que las fortalezas, oportunidades, debilidades y amenazas - DOFA, contenidas en el Plan Estratégico Institucional 2020 – 2021 del 21/07/2020, no se evidencian modificadas en la actualización realizada al 30/09/2021 y al respecto adicional a lo planteado por la norma ISO 9001:2015 en la que se indica que "*la organización* ***debe realizar el seguimiento y la revisión de la información*** *sobre estas cuestiones externas e internas*"; en la guía para la administración del riesgo y el diseño de controles en Entidades Públicas, se establece que "*una vez determinados estos lineamientos básicos,*

***es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos y planeación institucional, entre otros aspectos, esto permite conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general****" (resaltado fuera de texto).*

Lo anterior, en concordancia con la norma ISO 31000:2018 – *Administración / Gestión de Riesgos – Lineamientos Guía, que sirve de referencia conforme a la Guía de Administración de Riesgos en Entidades Públicas del DAFP*, en la cual se establece como uno de los principios para la gestión efectiva y eficiente de la gestión de riesgos que sea **Dinámica**, lo anterior, toda vez que "*Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos interno y externo de la organización. La administración/gestión de riesgos anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna*".

- Adicionalmente se verificó su inclusión en el modelo de Operación por Procesos de la Entidad y se evidenció como parte del Proceso de Control Fiscal; incluido como un Tema Asociado; veamos:

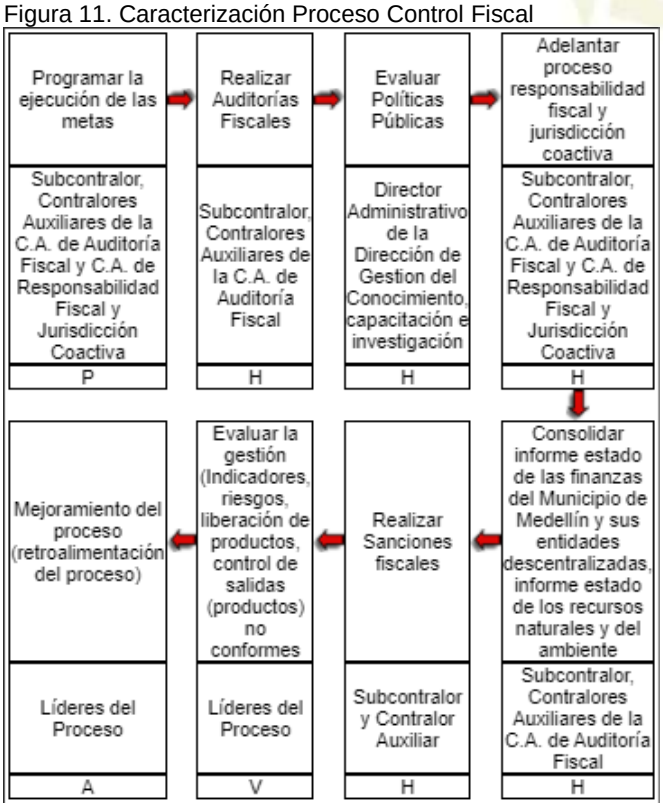
Figura 10. Modelo de operación por procesos




**Fuente:** Mapa de Procesos – Isolución, Código: MP-GE-PL-001, Versión 6

Al verificar la caracterización del proceso de Control Fiscal, el objetivo corresponde a: "*Ejercer la vigilancia y el control fiscal, a través de la realización de auditorías, elaboración de los informes de ley, estableciendo la responsabilidad fiscal, imponiendo las sanciones fiscales y ejerciendo la jurisdicción coactiva, para garantizar la defensa y protección del patrimonio público*"; cuyo alcance "*Inicia con la planificación de las actividades requeridas para la realización de las auditorías fiscales, consolidación financiera y ambiental y termina con los informes correspondientes, las sanciones fiscales y la responsabilidad fiscal y jurisdicción coactiva*"; **sin que en esta se incluya lo relacionado con la Evaluación de las Políticas Públicas**; aunque se encuentra como un tema asociado en el mapa de procesos para el proceso de Control Fiscal; así como en la caracterización del proceso; veamos:

Figura 11. Caracterización Proceso Control Fiscal




**Fuente:** Caracterización Procesos Control Fiscal – Isolución, Código: C-CF-001, Versión 4

Por último, por Resolución 152 del 07/05/2020, "*Por medio de la cual se crea el Grupo de Seguimiento y Evaluación de Políticas Públicas en la Contraloría General de Medellín y* ***se determina la formulación de la metodología para***

***evaluar las Políticas Públicas del Municipio de Medellín***", en su artículo tercero se definió la "*metodología y el proceso para la evaluación de las Políticas Públicas del Municipio de Medellín…*"; quedando como anexo a dicha Resolución; siendo verificado en Isolución / Listado Maestro de Documentos la inclusión de la Metodología *Seguimiento y Evaluación Políticas Públicas*, Código: G-GTC-GC-002, Versión 1.

Adicional a lo anterior, al verificar la responsabilidad por la ejecución de la meta relacionada con el Seguimiento y Evaluación de Políticas Públicas para la vigencia 2021, se evidenció que se tenía en el Plan de Acción Institucional una meta relacionada con la "*Evaluación integral de las políticas públicas u otros temas de interés*", que tiene como meta la "*Evaluación y seguimiento al 70% de las Políticas Públicas o temas públicos de interés priorizados correspondiente a cuatro temáticas específicas*", la cual se encuentra asignada a la Dirección de Gestión del Conocimiento, Capacitación e Investigaciones y como corresponsable la Contraloría Auxiliar de Apoyo Técnico.

No obstante lo anterior, el Proceso de Control Fiscal, tiene como responsables al Subcontralor y Contralores Auxiliares de Auditoria Fiscal y al verificar el Acuerdo Municipal 087 de 2018, "*por el cual se modifica la estructura organizacional de la Contraloría General de Medellín y se señalan los objetivos y funciones de sus dependencias*", se establece como objetivo para la Contraloría Auxiliar de Apoyo Técnico, el "*orientar y apoyar al Despacho del Contralor en el cumplimiento de las funciones constitucionales y legales, mediante la generación de propuestas y recomendaciones que contribuyan a la toma de decisiones, y al logro de la misión institucional*" y en el caso de la Dirección de Gestión del Conocimiento, Capacitación e Investigaciones, su objetivo consiste en "*generar, incorporar y transferir conocimiento de los funcionarios, fortaleciendo las competencias funcionales y comportamentales para mejorar su desempeño y fomentar la investigación, estudios y análisis con enfoque institucional para el logro de los objetivos de la entidad*"; con los riesgos que esto puede implicar.

### 7.1.2 Identificación de los Puntos de Riesgo

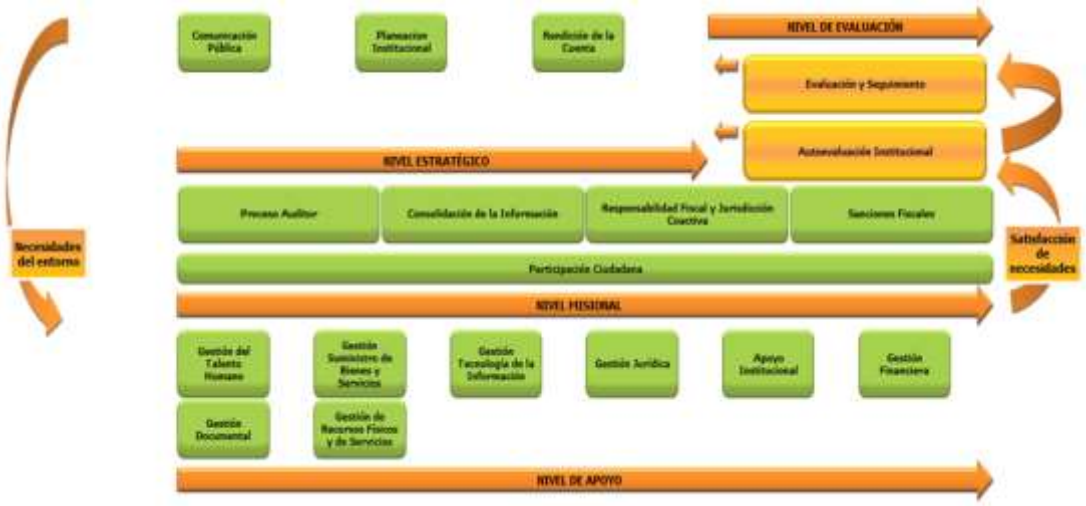
Conforme a la Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas, Versión 5, se establece en relación con los puntos de riesgo, que corresponden a las "*actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y*

*deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo*" y para mayor precisión, en las siguientes sesiones de capacitación realizada por Servidores Públicos de la Función Pública, se plantea lo siguiente:

- En capacitación del 06/05/2021 y que puede ser consultada en la ruta: https://www.youtube.com/watch?v=Rb-eclWKZdk, se manifiesta que: *"esto toca entenderlo* ***desde la cadena de valor y no como el área sola,…, hay algunos procesos sobre todo los procesos de apoyo, …*** *que están completamente interrelacionados, … por ejemplo en un proceso de gestión de recursos, pues seguramente hay unos procesos misionales que me afectan en este proceso, cuando yo estoy en gestión de recursos seguramente ese proceso afecta la gestión financiera, la gestión financiera pues seguramente también afecta esa gestión contable, entonces* ***necesito entender eso en términos de una cadena de valor y no como áreas sueltas porque ahí empiezan los problemas…****"*

  Al respecto, previa a la modificación realizada al mapa de procesos de la Entidad, el modelo de operación por procesos de la entidad tenía establecidos 4 niveles: Estratégico, Misional, de Apoyo y de Evaluación y estaba compuesto por 18 procesos, con 40 procedimientos, 28 documentos de apoyo y el Manual del Sistema Integrado de Gestión, entre otros; siendo importante tener en cuenta que cada uno de los procesos contaba con su respectiva caracterización y documentación relacionada, entre otras procedimientos y documentos de apoyo; tal como se presenta a continuación:

Figura 12. Mapa de Procesos Institucional




**Fuente:** Informe de Evaluación al SCI año 2015 – Oficina de Control Interno

Sin embargo, durante la vigencia 2016, la entidad avanza en la revisión del modelo de operación por procesos y pasa de tener 18 procesos a 6 procesos; tal como se presentó anteriormente; y lo que anteriormente fuera considerado como un proceso, pasó a documentarse como un procedimiento / Guía o Manual; lo que implicó que las interrelaciones identificadas entre los diferentes proceso; así como las actividades requeridas para la ejecución de los mismos fueran desconocidas; por lo que actualmente en la entidad no se presenten las interrelaciones entre procesos como gestión financiera, gestión de suministro de bienes y servicios, gestión de recursos físicos y de servicios; entre otros, toda vez que hacen parte del mismo proceso y no fueron documentados como subprocesos.

En relación con el mantenimiento y diseño de los procesos operativos de la CGM, tal como se manifestó anteriormente, el Jefe de la Oficina de Control Interno, al respecto planteó lo siguiente en Consejo de Dirección, Acta 05 del 27/05/2021, *"la OCI ha evidenciado que falta una mayor claridad en la secuencia de las actividades que interactúan, la responsabilidad que se asigna a cada una de ellas y los requerimientos que hay entre sí, para su suficiente funcionamiento; considera que el alcance de los procesos dada la magnitud que hoy tienen, cobijan actividades que pueden distar de su objeto, de su naturaleza, de su responsabilidad, inclusive de su riesgo, notando dificultad en su administración"*

- En capacitación del 29/09/2021 y que puede ser consultada en la ruta: https://www.youtube.com/watch?v=oM9M_BWTGn8&t=5224s, se plantea que "***los puntos de riesgo son esas actividades dentro del flujo operativo del proceso****, es decir dentro de la caracterización del proceso; recuerden que la caracterización del proceso nosotros documentamos, ese flujo operativo del proceso* ***donde existe evidencia****, es decir,* ***ya hay evidencia que un riesgo materializado históricamente o anteriormente o que los funcionarios que están en el ejercicio identificación de riesgo puedan llegar a tener indicios de que allí puede ocurrir un evento de riesgo operativo*** *y pues debe mantenerse bajo control, es decir debe identificarse como un riesgo y quizás este sea uno de los elementos más importantes para la gestión del riesgo"*

Para efectos de analizar lo planteado frente a los puntos de riesgo, en relación con los riesgos materializados históricamente, se procedió a consultar en Isolución / módulo de mejora, el consolidado de hallazgos reportados por la Auditoría General de la República, evidenciándose desde el 2015 a 2021, un total de 124 hallazgos, de los cuales 103 ya han sido evaluados por dicha entidad en la efectividad del plan

de mejoramiento diseñado para su tratamiento; siendo efectivo para el 75,7% de los hallazgos gestionados; a continuación se presenta el consolidado, veamos:

Tabla 4. Consolidado de Hallazgos AGR 2015 - 2021

| Procedimiento Relacionado | Efectividad | | | Total General | Porcentaje de Participación |
|---|---|---|---|---|---|
| | No | Si | Sin cierre | | |
| Planeación estratégica | | 1 | | 1 | 0,8% |
| Gestión Jurídica | | 1 | | 1 | 0,8% |
| Rendición de cuenta | 3 | | 1 | 4 | 3,2% |
| Gestión Documental | | | 1 | 1 | 0,8% |
| Auditoría Fiscal | | | 2 | 2 | 1,6% |
| Indagación preliminar | 2 | 8 | 2 | 12 | 9,7% |
| Proceso Responsabilidad Fiscal | 7 | 6 | 3 | 16 | 12,9% |
| Proceso jurisdicción coactiva | | 8 | 1 | 9 | 7,3% |
| Gestión PQRSD | | 7 | 1 | 8 | 5,6% |
| Proceso talento humano | 1 | | 1 | 2 | 1,6% |
| Capacitación | | | 1 | 1 | 0,8% |
| Incapacidades | 1 | 1 | 1 (1) | 3 | 2,4% |
| Vivienda | | | 1 (1) | 1 | 0,8% |
| Viáticos | | 2 | | 2 | 1,6% |
| Proceso contable | 8 | 15 | 1 | 24 | 19,4% |
| Proceso financiero-Tesorería | 1 | | | 1 | 0,8% |
| Presupuesto | | 2 | | 2 | 1,6% |
| Tesorería | | 2 | | 2 | 1,6% |
| Gestión de Bienes y Servicios | | 1 | | 1 | 0,8% |
| Proceso contratación | 2 | 23 | 4 | 29 | 23,4% |
| Cobro Coactivo PAC | | | 1 | 1 | 0,8% |
| Plan de Mejoramiento | | 1 | | 1 | 0,8% |
| Evaluación y Seguimiento | | 1 | | 1 | 0,8% |
| **Total general** | **25** | **78** | **21** | **124** | **100,0%** |

**Fuente:** Aplicativo Isolución / Modulo de Mejora – Construcción Propia

**Nota:** De los 21 hallazgos que se encuentran pendientes de cierre, 19 corresponden a la vigencia 2021 y dos (2) a la vigencia 2020 y están relacionados con

incapacidades y vivienda; adicionalmente, no se incluyeron las acciones correctivas 432 y 433.

En el consolidado anterior, se puede observar que de los 124 hallazgos, un total de 37 están relacionados con el Proceso de Responsabilidad Fiscal y Jurisdicción Coactiva, 29 con Contratación y 24 con el proceso contable; representando el 73% de los hallazgos generados a la Entidad.

En relación con los hallazgos generados por la Auditoría General de la República, se pudo evidenciar que en la vigencia 2021, se generaron dos (2) hallazgos para el proceso auditor, uno (1) para Gestión Documental, uno (1) para capacitación y uno (1) para Cobro Coactivo PAC; siendo importante tener en cuenta que en vigencias anteriores no se habían presentado; veamos:

- *"…La Contraloría tiene pendientes por evaluar 13 cuentas de la vigencia 2019 y 10 del 2018, que no fueron objeto de proceso auditor en su modalidad Regular. Con lo anterior, se incumple lo dispuesto en la Carta Política. 268, núm. 2º y 272, inc. 6º…"*
- *"…En los 10 informes evaluados, se evidencian deficiencias en la estructuración de las observaciones y de los hallazgos, presentando de manera generalizada y descriptiva los requisitos para configurar los hallazgos, no reflejando así los elementos y soportes suficientes en la configuración de los mismos…".*
- *"…Con Resolución nro. 028 del 18 de febrero de 2019, la Contraloría adoptó el manual de procedimiento de cobro coactivo PAC -CÓDIGO: P-GRI-GF-005; sin embargo, se observa que en el mismo se establecen actividades, como lo son la solicitud de "concepto jurídico" no establecidas en la norma que reglamenta la materia y adicionalmente, se evidencian riesgos frente al cumplimiento de las actividades procesales, propias por su naturaleza de oficinas con perfiles con conocimientos en derecho, que garantizan el cumplimiento y aplicación adecuada de las mismas…".*
- *"…La Contraloría no hizo entrega de algunos documentos requeridos para el proceso auditor de la AGR dentro del proceso de Participación Ciudadana…".*

Sin que se evidencie que como resultado de lo anterior se hayan revisado y ajustado los controles establecidos para los riesgos o se hayan identificado nuevos riesgos de ser pertinente.

Entre los temas relacionados con los hallazgos consolidados por la AGR, se encuentran los siguientes:

- Deficiencias en registro, depuración de saldos, recobro de incapacidades; así como saldos prescritos y deficiente gestión de reconocimiento de incapacidades ante las diferentes EPS.
- Extemporaneidad de la publicación en el SECOP.
- Configuración del fenómeno jurídico de la caducidad y prescripción de la acción fiscal; así como falta de oportunidad para iniciar las indagaciones preliminares.
- No vinculación de las compañías aseguradoras, no investigación de bienes en procesos de responsabilidad fiscal y no decreto de medidas cautelares
- Los hechos investigados no guardan conexidad ni unidad procesa
- Debilidades en la etapa probatoria; así como dilación procesal y falta de oportunidad para decidir en procesos de responsabilidad fiscal.
- Incumplimiento del término legal para tomar decisión de fondo
- Falta de conciliación entre áreas de presupuesto y contabilidad; así como con activos fijos
- Inexactitud en saldos; ajustes contables sin documentos soportes de identificación de diferencias, imprecisión de registro contable;
- Falta de provisión de sentencia y pago sin observarse el reconocimiento en la cuenta Pasivos estimados.
- Errores y fallas en el registro y depuración de la información contable
- Pagos que no fueron causados en el sistema contable.
- Inconsistencias en la información: conciliación de activos fijos, registros dobles, falta de causación oportuna de los hechos económicos y falta de cálculo del deterioro en cuentas por cobrar
- Inconsistencias en la presentación de información exógena
- Registro de los movimientos contables bajo el régimen anterior
- Saldos en cuentas bancarias pendientes por conciliar
- Inconsistencias en la documentación legal exigida
- Indebida justificación de la descripción de la necesidad que se pretendía satisfacer.
- Incumplimiento del objeto contractual
- Incumplimiento en la selección de la modalidad de contratación
- Debilidades en la labor de supervisión relacionadas con la omisión de funciones y actuaciones oportunas.
- Deficiencias en la verificación de las características tributarias consignadas en el Registro Único Tributario
- Vulneración del régimen legal de inhabilidades e incompatibilidades
- No contestar las excepciones con oportunidad en Jurisdicción Coactiva
- No abrir cuaderno de medidas cautelares

- Inadecuada conformación del título y falta de ejecutoriedad y ejecutividad
- Inconsistencias en la rendición de la cuenta a la AGR
- No cumplimiento total de la comisión por parte de un funcionario
- No contar con un sistema de información que garantice el proceso de la información de manera eficiente para el programa de vivienda.
- Indebida comunicación al denunciante sobre el traslado por competencia de una PQRSD e inconsistencias en la respuesta de fondo.
- Trámite inadecuado del archivo de denuncias por desistimiento

Sin embargo, es importante tener en cuenta que la norma ISO 9001:2015, en relación con las no conformidades y acción correctiva, establece en el numeral 10.2.1, literal e y f, que "*si fuera necesario,* ***actualizar los riesgos y oportunidades determinados durante la planificación***" y "*si fuera necesario,* ***hacer cambios al sistema de gestión de la calidad***"; sin embargo, existen temas, por ejemplo lo relacionado con el Proceso de Responsabilidad Fiscal y Jurisdicción Coactiva, en el que se tiene el riesgo "Posibilidad de afectación económica y reputacional por la prescripción de los procesos de responsabilidad fiscal, debido a la inactividad procesal"; sin embargo, no se visualizan riesgos relacionados con:

- La no vinculación de las compañías aseguradoras, no investigación de bienes en procesos de responsabilidad fiscal y no decreto de medidas cautelares.
- Los hechos investigados no guardan conexidad ni unidad procesa
- Debilidades en la etapa probatoria; así como dilación procesal y falta de oportunidad para decidir en procesos de responsabilidad fiscal.
- Incumplimiento del término legal para tomar decisión de fondo.

Situación similar se tiene para algunos temas que han sido objeto de hallazgos por parte de la Auditoría General de la República, a los cuales no se les ha relacionado riesgos o los controles diseñados son muy generales y no específicos para éstos; veamos:

- Deficiencias en registro, depuración de saldos, recobro de incapacidades; así como saldos prescritos y deficiente gestión de reconocimiento de incapacidades ante las diferentes EPS.
- Extemporaneidad de la publicación en el SECOP.
- Inexactitud en saldos; ajustes contables sin documentos soportes de identificación de diferencias;
- Falta de provisión de sentencia y pago sin observarse el reconocimiento en la cuenta Pasivos estimados.

- Inconsistencias en la información: conciliación de activos fijos, registros dobles, falta de causación oportuna de los hechos económicos y falta de cálculo del deterioro en cuentas por cobrar
- Inconsistencias en la presentación de información exógena
- Registro de los movimientos contables bajo el régimen anterior
- Saldos en cuentas bancarias pendientes por conciliar
- Debilidades en la labor de supervisión relacionadas con la omisión de funciones y actuaciones oportunas.
- Deficiencias en la verificación de las características tributarias consignadas en el Registro Único Tributario
- Vulneración del régimen legal de inhabilidades e incompatibilidades
- No cumplimiento total de la comisión por parte de un funcionario
- No contar con un sistema de información que garantice el proceso de la información de manera eficiente para el programa de vivienda.

Dentro de los planes de mejoramiento formulados durante las diferentes vigencias, se han evidenciado la revisión de controles relacionados con algunos procedimientos y los ajustes a la documentación; lo que ha conllevado a que los hallazgos no se vuelvan a presentar; entre otras, relacionados con la gestión financiera y contable.

Adicionalmente, en la revisión realizada, se pudo evidenciar que los 25 hallazgos, cuyos tratamientos fueron considerados no efectivos, están relacionados con los procesos, conforme se detalla a continuación:

Tabla 5. Hallazgos AGR no efectivos por proceso

| **Procedimiento Relacionado** | **Año** | | | | | **Total** |
|---|---|---|---|---|---|---|
| | **2016** | **2017** | **2018** | **2019** | **2020** | |
| Incapacidades | | 1 | | | | **1** |
| Indagación preliminar | 1 | 1 | | | | **2** |
| Proceso contable | | | 8 | | | **8** |
| Proceso contratación | | | 2 | | | **2** |
| Proceso financiero-Tesorería | | | 1 | | | **1** |
| Proceso Responsabilidad Fiscal | | 6 | | | 1 | **7** |
| Proceso talento humano | | 1 | | | | **1** |
| Rendición de cuenta | | | 1 | 1 | 1 | **3** |
| **Total general** | **1** | **9** | **12** | **1** | **2** | **25** |

**Fuente:** Aplicativo Isolución / Modulo de Mejora – Construcción Propia

Es importante tener en cuenta que uno de los hallazgos que ha sido reiterativo en los últimos 3 años, ha sido lo relacionado con la Rendición de la Cuenta a la Auditoría General de la República; adicionalmente, que en los hallazgos analizados sólo se incluyeron los que fueron generados por la Auditoría General de la República y no por las Evaluaciones Independientes realizadas por la Oficina de Control Interno.

En relación con las evaluaciones independientes e informes de ley realizados por la Oficina de Control Interno, se han evidenciado aspectos que son susceptibles de riesgos y en los cuales no se tienen identificados riesgos, entre otras los siguientes:

- Gestión del Sistema de Información y Gestión del Empleo Público - SIGEP
- Sistema de Gestión de la Seguridad y Salud en el Trabajo – SG SST.
- Planes de Mejoramiento
- Transparencia y Acceso a la Información Pública
- Derechos de autor

Adicionalmente en las Actas del Consejo de Dirección, se evidencian temas que son susceptibles de riesgos; entre otras:

- Plan Estratégico de Seguridad Vial – PESV
- Plan Institucional de Gestión Ambiental – PIGA
- Certificación Anual de Gestión por parte de la Auditoría General de la República a la Contraloría General de Medellín
- Plan de Movilidad Empresarial Sostenible – Plan MES
- Gestión integral del programa de vivienda
- Registro de base de datos ante la Superintendencia de Industria y Comercio – SIC

Por último, no se evidencian riesgos y controles relacionados con la continuidad del negocio, ni riesgos de fraude.

### 7.1.3 Identificación de Áreas de Impacto

En relación con esta fase, la metodología establece que "*el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo*" y al verificar los diferentes riesgos que hacen parte de la matriz de riesgos institucional, se evidencia que en todos se indica el impacto

conforme a lo establecido en la Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas, versión 5.

No obstante lo anterior, en algunos casos no se profundiza en el impacto que puede generar la materialización del riesgo; por ejemplo para el riesgo "*Posibilidad de afectación reputacional, por incumplimiento de metas y objetivos, debido a la falta de seguimiento a las metas trazadas por parte de los líderes de los procesos*"; el incumplimiento de metas puede implicar para la Entidad, la pérdida de la certificación por parte de la Auditoría General de Republica, y la posible intervención administrativa por parte de la Contraloría General de la República, debido a que el índice AuditeCT para la contraloría, sea menor al puntaje crítico de certificación anual, conforme a la metodología definida por la Auditoría General de la República.

Adicionalmente, en el caso del riesgo relacionado con la "*Posibilidad de afectación reputacional, por la pérdida de información documentada, debido a omitir la entrega de los inventarios documentales, la no devolución de los documentos prestados o causas naturales*", la Ley 594 de 2000, establece en el artículo 35 que "*…el incumplimiento de las órdenes impartidas conforme al presente literal será sancionado por la autoridad que las profiera, con multas semanales sucesivas a favor del tesoro nacional, departamental, distrital o municipal, según el caso, de hasta veinte (20) salarios mínimos legales mensuales, impuestas por el tiempo que persista el incumplimiento"; por lo que la pérdida de información documentada, no sólo genera una posible afectación reputacional…*"

Sin embargo, en la fase de Descripción del Riesgo, se analizará la estructura del riesgo, toda vez que se evidencia debilidades en su estructuración; sin embargo, en esta fase no se busca analizar si el riesgo está o no descrito de manera adecuada.

### 7.1.4 Identificación de Áreas de Factores de Riesgo

De conformidad con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, "*Los factores relacionados son una guía,* ***cada entidad puede analizar los que considere de acuerdo con la complejidad propia de cada entidad y con sector en el que se desenvuelve****, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo*"; sin embargo, al verificar la Política de Administración de Riesgos de la Entidad, solo se plantea "…los factores de riesgos como procesos, talento humano, tecnología, infraestructura y eventos externos…"; sin que se dé

información adicional sobre su definición y una descripción de dichos factores o que se hayan considerado otros adicionales, conforme a lo planteado en la guía. (Resaltado fuera de texto).

### 7.1.5 Descripción del Riesgo

Con el fin de evaluar la aplicación de esta fase en la gestión de riesgos para la vigencia 2021, inicialmente se realizó una comparación para algunos riesgos identificados en la vigencia 2020 frente a los de la vigencia 2021 y se pudo evidenciar lo siguiente:

**Proceso:** Control Fiscal

- **Descripción del Riesgo vigencia 2021:**
  **Impacto:** "*Reputacional",*
  ***Causa Inmediata:*** *"Producir* ***evaluaciones sin rigor técnico*** *con resultados errados, quejas de las partes interesadas e investigaciones de entes reguladores y disciplinarios".*
  ***Causa Raíz:*** *"Desconocimiento de los procesos, riesgos y normativa de la entidad auditada;* ***debilidades en la planeación de auditorías en cuanto al alcance, conformación de equipos, tiempos, temas a auditar*** *y perfil del equipo auditor; Inoportunidad, insuficiencia o mala calidad de la información rendida; deficiencias de control y supervisión en el desarrollo del proceso auditor; debilidades en la evaluación de los principios fiscales y en la formulación y soporte de los posibles hallazgos con incidencia fiscal; emisión de informes que contienen conclusiones y/o hallazgos que no concuerdan con la realidad de la gestión y resultados del sujeto de control*".

- **Nombre del Riesgo 2020:** "***Auditorías sin rigor técnico***"
  **Consecuencias:** "*Generar pérdida de confianza de la entidad, afectando su reputación, Incumplimiento en las metas y objetivos institucionales, Reproceso de actividades y aumento de carga operativa,* ***Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad*** *o implican investigaciones internas disciplinarias*".
  **Causas:**
  - ✓ "*Debilidades en la planeación de auditorías en cuanto al alcance, conformación de equipos, tiempo, temas a auditar con experticia técnica de los directivos y equipo auditor*"

- ✓ "*Desconocimiento de los procesos, riesgos y normativa de la entidad auditada*"
- ✓ "*Aplicación inadecuada del procedimiento de auditoría fiscal por falta de control efectivos (validación de hallazgos)* "
- ✓ "*Inoportunidad o falta de información adicional a la rendición anual requerida para el desarrollo del ejercicio de control fiscal*"

- **Comentarios OCI:** Al realizar el cruce para el riesgo identificado durante la vigencia 2020 y 2021 para el proceso de Control Fiscal en lo que tiene que ver con las auditorías fiscales, se evidenció lo siguiente:

  - ✓ Se tiene relación para ambas vigencias y en términos generales está relacionado con evaluaciones sin rigor técnico
  - ✓ Similar la redacción de las consecuencias para el riesgo en 2020 frente al impacto y la causa inmediata del riesgo en 2021, teniendo elementos adicionales en 2020, como es una posible "***…denuncia…***" y "…***demanda de largo alcance para la entidad"***
  - ✓ *Frente a la causa raíz para 2021, entre otras, no se incluye lo relacionado con el posible "Desconocimiento de los procesos, riesgos y normativa de la entidad auditada"; así como la "Aplicación inadecuada del procedimiento de auditoría fiscal…" que fueran identificadas como causas durante la vigencia 2020.*

**Proceso:** Control Fiscal

- **Descripción del Riesgo vigencia 2021:**
  **Impacto:** "*Económico y Reputacional"*
  ***Causa Inmediata:*** *"Caducidad de la acción fiscal en los hallazgos fiscales, en las indagaciones preliminares que procedan de las denuncias ciudadanas y del traslado de otras entidades"*
  ***Causa Raíz:*** *"Inactividad procesal para calificar los Hallazgos Fiscales y las Indagaciones Preliminares e iniciar los procesos de responsabilidad fiscal*".

- **Nombre del Riesgo 2020:** "***Caducidad después de comisión o prescripción***"
  **Consecuencias:** "*Generar pérdida de confianza de la entidad, afectando su reputación, Investigaciones penales, fiscales o disciplinarias.*".
  **Causas:**
  - ✓ "*Inactividad procesal a partir del auto de apertura en el proceso ordinario y/o inactividad procesal a partir del auto de apertura e imputación en el proceso verbal*"

- ✓ ”*No revisar la fecha de ocurrencia de los hechos para iniciar la indagación preliminar o el proceso de responsabilidad fiscal*”

- **Comentarios OCI:** Al realizar el cruce para el riesgo identificado durante la vigencia 2020 y 2021 para el proceso de Control Fiscal en lo que tiene que ver con la Responsabilidad Fiscal, se evidenció lo siguiente:
  - ✓ Se tiene relación para ambas vigencias y en términos generales está relacionado con la caducidad de la acción fiscal
  - ✓ Al analizar la causa inmediata para el riesgo de la vigencia 2021, se evidencia que no se incluye la consecuencia identificada durante la vigencia 2020 y que corresponde a las posibles “…*investigaciones penales, fiscales y disciplinarias*”, que podrían afectar la reputación de la entidad; adicionalmente se plantea en relación con la caducidad que sea para “…indagaciones preliminares que procedan de las denuncias ciudadanas y del traslado de otras entidades…”; sin tener en cuenta que igualmente se pueden generar principalmente como resultado del proceso auditor adelantado por las Contralorías Auxiliares de Auditoría Fiscal.
  - ✓ *Frente a la causa raíz para 2021 y las causas identificadas durante 2020, no se evidencia relación; sin embargo, en ninguno de los dos casos se profundiza en que puede ser lo que genere la posible caducidad del proceso de la acción fiscal.*

**Proceso:** Participación Ciudadana

- **Descripción del Riesgo vigencia 2021:**
  **Impacto:** “*Reputacional”*
  ***Causa Inmediata:*** *“Inadecuadas e inoportunas respuestas de las PQRSD a los ciudadanos”*
  ***Causa Raíz:*** *“Inaplicabilidad del Manual de Tramite de las PQRSD*”.

- **Nombre del Riesgo 2020:** “*Respuestas inadecuadas y/o inoportunas a los requerimientos realizados por la ciudadanía*”
  **Consecuencias:** “*Generar pérdida de confianza de la entidad, afectando su reputación, Sanción por parte del ente de control u otro ente regulador, Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad o implican investigaciones internas disciplinarias*”.
  **Causas:**
  - ✓ “*La no aplicación del procedimiento de las PQRSD*”
  - ✓ ”*Falta de análisis crítico o lectura de la solicitud realizada por el ciudadano*”

- **Comentarios OCI:** Al realizar el cruce para el riesgo identificado durante la vigencia 2020 y 2021 para el proceso de Participación Ciudadana en lo que tiene que ver con la gestión de las PQRSD, se evidenció lo siguiente:
  - ✓ Se tiene relación para ambas vigencias y en términos generales está relacionado con las "*Inadecuadas e inoportunas respuestas de las PQRSD…"*
  - ✓ Al analizar la causa inmediata para el riesgo de la vigencia 2021, se evidencia que no se incluye la consecuencia identificada durante la vigencia 2020 y que corresponde a posible "…*Sanción por parte del ente de control u otro ente regulador*", que podrían afectar la reputación de la entidad; adicionalmente se plantea posible "…*denuncia ante los entes reguladores o una demanda de largo alcance para la entidad o implican investigaciones internas disciplinarias*".
  - ✓ *Frente a la causa raíz para 2021 y las causas identificadas durante 2020, en términos generales son la misma; sin embargo, en 2020 se plantea que también puede ser por "Falta de análisis crítico o lectura de la solicitud realizada por el ciudadano"; sin que se evidencie que se haya profundizado en el análisis de las causas, entre otras que puede estar relacionado con que no se gestionen la totalidad de las PQRSD por que no se radiquen en la ventanilla única.*

    Adicionalmente, no se evidencian causas relacionadas con la gestión de denuncias por parte del proceso de Control Fiscal, cuando estás proceden de PQRSD.

**Proceso:** Gestión del Talento Humano y del Conocimiento

- **Descripción del Riesgo vigencia 2021:**
  **Impacto:** "*Reputacional"*
  ***Causa Inmediata:*** *"Reclamaciones de los servidores públicos por la nómina"*
  ***Causa Raíz:*** *"Inconsistencia en la liquidación de la bonificación por servicios prestados en el sistema de nómina*".

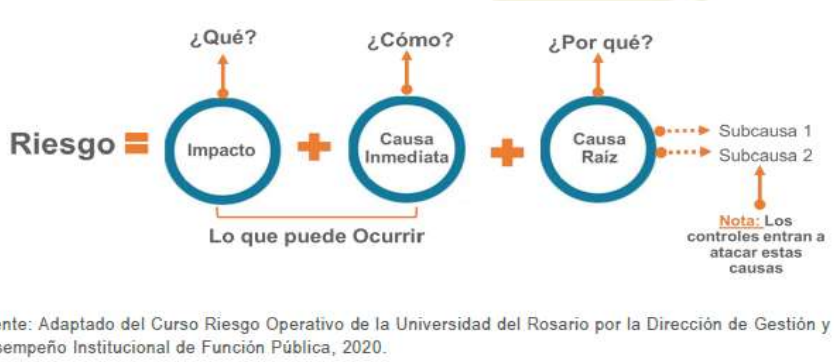
  **Impacto:** "*Económico y Reputacional"*
  ***Causa Inmediata:*** *"Reclamaciones de los servidores públicos y las entidades prestadoras de salud, Fondo de Pensiones y Cesantías"*
  ***Causa Raíz:*** *"Inconsistencia en la liquidación de la Seguridad Social*".

- **Nombre del Riesgo 2020:** "*Inexactitud en la liquidación de nóminas y prestaciones sociales*"
  **Consecuencias:** "*Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, reproceso de actividades y aumento de carga operativa*".
  **Causas:**
  - ✓ "*Liquidación manual de nómina y prestaciones sociales*"

- **Comentarios OCI:** Al realizar el cruce para el riesgo identificado durante la vigencia 2020 y 2021 para el proceso de Gestión del Talento Humano y del Conocimiento en lo que tiene que ver con la liquidación de la nómina y las prestaciones sociales, se evidenció lo siguiente:
  - ✓ Si bien para la vigencia 2021 se tienen 2 riesgos identificados, en la vigencia 2020 se planteó como uno (1) solo y está relacionado con la liquidación de nómina y prestaciones sociales
  - ✓ Al analizar la causa inmediata para el riesgo de la vigencia 2021, se evidencia que no se incluye la consecuencia identificada durante la vigencia 2020 y que corresponde, entre otras, a posible "…*Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador*.
  - ✓ Frente a la causa raíz para 2021 y las causas identificadas durante 2020, para la vigencia 2021 se estableció que se debe a inconsistencias en la liquidación de la bonificación por servicios prestados y de seguridad social respectivamente; sin embargo, durante la vigencia 2020, se había identificado que podría deberse a la *"liquidación manual de nómina y prestaciones sociales",* siendo relacionado con el aplicativo utilizado para la liquidación; sin embargo, esta causa no se tuvo en cuenta en 2021; adicionalmente, no se profundiza en las sub causas relacionadas con la liquidación de nómina y prestaciones sociales, conforme a la guía.

Adicionalmente, se realizó el análisis de la Estructura propuesta para la Redacción del Riesgo conforme a la metodología establecida por la Función Pública, la cual en términos generales corresponde a la siguiente:

Figura 13. Estructura para la redacción de Riesgos propuesta por el DAFP




Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**Fuente:** Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 5, Función Pública

En la aplicación de la metodología, es importante tener en cuenta los siguientes conceptos definidos en la guía:

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Al verificar el cumplimiento de lo establecido en la Guía para la estructuración de algunos riesgos en la Entidad se pudo evidenciar, entre otras, lo siguiente:

Tabla 6. Verificación Riesgos Institucionales

| Impacto | Causa Inmediata | Causa Raíz | Observaciones Oficina de Control Interno |
|---|---|---|---|
| Reputacional | Incumplimiento de metas y objetivos | Falta de seguimiento a las metas trazadas, por parte de los líderes de los procesos. | La causa inmediata no corresponde y entre otras la posible afectación reputacional de la entidad se podría deber a la pérdida de la certificación por parte de la Auditoría General de Republica, y la posterior intervención administrativa por parte de la Contraloría General de la República, |

| Impacto | Causa Inmediata | Causa Raíz | Observaciones Oficina de Control Interno |
|---|---|---|---|
| | | | debido a que el índice AuditeCT para la contraloría, sea menor al puntaje crítico de certificación anual, conforme a la metodología definida por la AGR. Adicionalmente, no se profundiza en las posibles causas y subcausas; que permitan posteriormente identificar con mayor claridad los controles requeridos. |
| Reputacional | Desactualización del SIG | Falta de seguimiento y revisión de los elementos del SIG por parte de los servidores de la entidad a fin de mantener el SIG actualizado. | La causa inmediata no corresponde y entre otras la posible afectación reputacional de la entidad se podría generar por la posible pérdida o suspensión de la certificación del SIG por parte del ente de certificación, debido, entre otras, a la desactualización del SIG e incumplimientos de los requisitos establecidos en la norma ISO 9001 vigente. |
| Económico y Reputacional | Declaratoria de nulidad y/o imposición de la obligación de resarcir | Elaboración de actos administrativos con fallas en la fundamentación fáctica y jurídica | Sin comentarios |
| Económico y Reputacional | Fallos judiciales con condenas patrimoniales en contra de la Entidad y de los sujetos de control. | Falta de verificación de términos procesales y judiciales | Sin comentarios en relación con el impacto y la causa inmediata; frente a la causas raíz no se profundiza en las posibles causas y subcausas; que permitan posteriormente identificar con mayor claridad los controles requeridos. |

| Impacto | Causa Inmediata | Causa Raíz | Observaciones Oficina de Control Interno |
|---|---|---|---|
| Reputacional | Uso inadecuado de los medios y canales de comunicación | Desacato de las directrices y políticas emitidas por la Oficina Asesora de Comunicaciones de la entidad. | La causa inmediata no corresponde y entre otras la posible afectación reputacional de la entidad se podría deberse conforme al riesgo identificado en 2020 a "*Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad o implican investigaciones internas disciplinarias"*<br>Adicionalmente se podrían considerar otros riesgos como:<br>* Posibilidad de pérdida reputacional por quejas masivas de los grupos de valor o de interés debido a la información no veraz y/o desactualizada en nuestra página web y redes sociales.<br>* Posibilidad de pérdida reputacional por demanda de los grupos de valor debido a la publicación de información clasificada.<br>Adicionalmente, no se profundiza en las causas y subcausas relacionadas. |
| Reputacional | Pérdida de información documentada | Omitir la entrega de los inventarios documentales, la no devolución de los documentos prestados, causas naturales | La causa inmediata no corresponde y entre otras la posible afectación reputacional de la entidad; que entre otras, podría deberse a sanciones por órganos de control; quejas de diferentes partes interesadas por solicitud de información que no sea entregada; entre otras.<br>Adicionalmente, no se profundiza en las causas y subcausas relacionadas. |
| Económico y Reputacional | Imposición de sanciones originadas en la contratación sin el cumplimiento de los requisitos legales | Fallas en la aplicación de controles en las etapas del proceso contractual | Se mezclan la causa inmediata y la causa raíz; siendo la causa inmediata la imposición de sanciones y la causa raíz, la contratación sin el cumplimiento de los requisitos legales.<br>Adicionalmente la causa raíz es muy general y no se identifican subcausas relacionadas. |
| Económico y Reputacional | Sanción del ente regulador por interpretación inadecuada o incumplimiento de la norma y | Fallas en la aplicación de los controles en la ejecución presupuestal | Se mezclan la causa inmediata y la causa raíz; adicionalmente las posibles sanciones disciplinarias, penales y fiscales se pueden dar, entre otras, por inconsistencias en la ejecución presupuestal o el incumplimiento de los principios presupuestales debido a la |

| Impacto | Causa Inmediata | Causa Raíz | Observaciones Oficina de Control Interno |
|---|---|---|---|
| | desaprovechamiento de los recursos financieros | | interpretación equivocada de la norma o el incumplimiento de esta. |
| Económico | Bienes muebles sin amparo en pólizas de seguros | Omisión en el reporte de bienes muebles adquiridos, para ser incluidos en la póliza de seguros | La causa inmediata no corresponde a lo establecido en la guía y entre otras, se podría presentar pérdida reputacional, por posibles sanciones o procesos disciplinarios que se puedan generar, entre otras, debido a la "*...disminución, perjuicio, detrimento, pérdida, uso indebido o deterioro de los bienes o recursos públicos, producida por una conducta dolosa, cometida por un servidor público...*"; así como por "*...no asegurar por su valor real los bienes del Estado...*" |
| Reputacional | Reclamaciones de los servidores públicos por la nomina | Inconsistencia en la liquidación de la bonificación por servicios prestados en el sistema de nómina. | En la revisión realizada con la Dirección de Talento Humano, se pudo evidenciar que el riesgo se enmarca en la liquidación de la bonificación debido a que el sistema Kactus está presentando inconsistencias al momento de liquidar la nómina definitiva dado que no está incluyendo este concepto y debe ser ingresado de manera manual.<br>Es importante verificar si la perdida reputacional se puede generar por inconsistencias en la liquidación de la nómina y prestaciones sociales, entre otros, porque el procedimiento tiene como objetivo el pago oportuno a los servidores y la liquidación de manera correcta de éstos.<br>Adicionalmente, se puede generar pérdida reputacional y sanciones económicas de entidades como la DIAN, debido, entre otras, a inconsistencias en la liquidación de las deducciones por retenciones en la fuente. |
| Reputacional | Inadecuada gestión del conocimiento | Inaplicación de los instrumentos de gestión | Es importante precisar cuál es la causa inmediata que podría implicar la posible pérdida reputacional para la Entidad; conforme a la metodología propuesta.<br>Adicionalmente profundizar en las causas y subcausas, de tal forma que se puedan definir posteriormente los riesgos relacionados. |
| Reputacional | Informe de Evaluación de Política Pública inapropiado | Falta de control en la aplicación del procedimiento para la evaluación de las políticas pública. | |

| Impacto | Causa Inmediata | Causa Raíz | Observaciones Oficina de Control Interno |
|---|---|---|---|
| Reputacional | Errores u omisiones en los informes de auditoría | Falta de idoneidad del equipo auditor, auditorías sin rigor técnico, incumplimiento del procedimiento auditor o por falta de información suficiente, relevante y útil. | |

**Fuente:** Matriz de Riesgos – Construcción Propia

Lo anterior, permite concluir que existen debilidades en la estructuración del riesgo, conforme a la metodología definida por la Función Pública; así mismo es necesario, profundizar en las subcausas, con el fin de poder posteriormente establecer los controles pertinentes.

Es importante tener en cuenta en la identificación del riesgo, lo planteado en la guía:

> "*No existen riesgos transversales, lo que pueden existir son causas transversales.*
> ***Ejemplo:*** *pérdida de expedientes.*
> *Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes*"

Por lo cual, es importante revisar aquellos riesgos que se pueden presentar en diferentes procesos; entre otros lo relacionado con la Rendición de la Cuenta y la gestión de las PQRSD; inclusive el ejemplo propuesto relacionado con Gestión Documental; por lo que es necesario que se identifiquen los controles que se deben ejecutar en cada proceso.

Adicionalmente, en la revisión realizada no se evidenciaron riesgos de fraude, que conforme a lo establecido en la metodología, entre otros, el fraude interno corresponde a "Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros" y que entre otros, podría estar relacionado con información financiera fraudulenta o apropiación indebida de activos.

### 7.1.6 Clasificación del Riesgo

En relación con la clasificación del riesgo, se pudo evidenciar que las categorías relacionadas corresponden para 21 riesgo a Ejecución y Administración de procesos, dos (2) a Fallas Tecnológicas y dos (2) a Usuarios, productos y prácticas organizacionales.

## 7.2 RIESGO DE CORRUPCIÓN

En relación con los riesgos de corrupción, no se incluye análisis específico, toda vez que en el Seguimiento realizado por la Oficina de Control Interno al Plan Anticorrupción y de Atención al Ciudadano, con corte al 30 de abril de 2021 y al 31 de agosto de 2021, se plantea lo siguiente: "*Una vez realizada la verificación de los seis riesgos de corrupción que la entidad tiene definidos, se observó que se diseñaron teniendo en cuenta criterios como: el responsable, segregación de funciones, periodicidad, el cómo se ejecuta y que soportes lo respaldan; además se diseñaron teniendo en cuenta la causa principal de cada riesgo. Por lo anterior* ***se concluye que cumplen con la estructura de un riesgo de corrupción****, es decir: son claros y precisos, la periodicidad del control es adecuada y cubren la mayoría de procesos de la entidad, no obstante lo anterior, se reitera desde esta oficina que el proceso de "Gestión del Talento Humano y del Conocimiento" no tiene riesgos asociados a los "riesgos de corrupción" tal como se indicó en el informe anterior*"

## 7.3 RIESGO DE SEGURIDAD DE LA INFORMACIÓN

La Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de 2020, establece en relación con los riesgos de Seguridad de la Información, que los pasos a seguir para la identificación de los riesgos corresponden a los siguientes:

- Identificación de los activos de seguridad de la información
- Identificación del riesgo
- Valoración del riesgo
- Controles asociados a la seguridad de la información

A continuación se analizan los pasos establecidos.

### 7.3.1 Identificación de los Activos de Seguridad de la Información

De acuerdo con la guía el "*para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso*", los cuales se definen como "*cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:*

*-Aplicaciones de la organización*
*-Servicios web*
*-Redes*
*-Información física o digital*
*-Tecnologías de información TI*
*-Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital*"

Adicionalmente, en la siguiente gráfica se presentan los pasos requeridos para identificar los activos; veamos:

Figura 14. Pasos para la identificación de activos


Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

**Fuente:** Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 5, Función Pública.

Al verificar la implementación de lo pertinente en la Entidad, se pudo evidenciar la identificación de 3 riesgos relacionados con la seguridad de la información; los cuales corresponden a los siguientes:

Tabla 7. Riesgos de Seguridad de la Información identificados en la CGM

| Riesgo | Activo | Descripción del Riesgo |
|---|---|---|
| Pérdida de la Confidencialidad | Sistemas de Información | La asignación errada de los derechos de acceso y la Gestión deficiente de las contraseñas por parte de los usuarios, lo cual causaría la pérdida de la confidencialidad de los sistemas de información |
| Pérdida de Integridad | Sistemas de Información | Asignación deficiente de permisos y perfiles de usuarios, generan la pérdida de integridad en los sistemas de información. |
| Pérdida de Disponibilidad | Software | Mantenimiento insuficiente del software y hardware genera la pérdida de disponibilidad de los servicios. |
| | Hardware | |

**Fuente:** Matriz de Riesgos de Seguridad de la Información al 26/10/2021 / Isolución

Sin embargo, conforme a la metodología se deben "listar los activos por cada proceso" y al verificar en la página web de la Entidad, en la Sección de Transparencia y Acceso a la Información Pública, se evidenció publicada en la sección de Datos Abiertos, el Registro de Activos de Información; veamos:

Figura 15. Publicación web Registro de Activos de Información


**Fuente:** Página web CGM

Al verificar en el Registro de Activos de Información, se identificó, que mediante Resolución 484 del 17/11/2020, se "*…modifica el Índice de Información Clasificada y Reservada y el Registro de Activos de Información, instrumentos de Gestión de la Información Pública*"; siendo parte de dichos activos de la información, entre otras, los siguientes:

Tabla 8. Activos de Información

| Categoría o Serie de la Información | Nombre o Título de la Información | Medio de Conservación y/o Soporte | Nombre del Responsable de la Información |
|---|---|---|---|
| Acciones Constitucionales | Acciones de Tutela | Físico | Oficina Asesora Jurídica |
| Acciones Constitucionales | Acciones Populares | Físico | Oficina Asesora Jurídica |
| Actas | Actas de Arqueo | Físico | Dirección de Recursos Físicos y Financieros |
| Actas | Comisión Regional de Moralización de Antioquia | Electrónico | Despacho Del Contralor |
| Actas | Acta de Comité Técnico de Auditoría | Físico | Subcontraloría |
| Actas | Acta de Comité de Adquisiciones de Bienes y Servicios | Físico | Secretaría General |
| Certificados | Certificado Presupuestal | Electrónico | Dirección de Recursos Físicos y Financieros |
| Certificados | Certificado Tributarios | Físico | Dirección de Recursos Físicos y Financieros |
| Circulares | Circulares | Electrónico | Secretaría General |
| Comprobantes | Movimientos Contables | Físico | Dirección de Recursos Físicos y Financieros |
| Comprobantes | Comprobantes de Causaciones | Físico | Dirección de Recursos Físicos y Financieros |
| Comprobantes | Comprobantes de Egresos | Físico | Dirección de Recursos Físicos y Financieros |
| Comprobantes | Comprobantes de Ingresos | Físico | Dirección de Recursos Físicos y Financieros |
| Comprobantes | Comprobantes de Movimientos Activos | Físico | Dirección de Recursos Físicos y Financieros |
| Conceptos | Conceptos Jurídicos | Físico y Electrónico | Oficina Asesora Jurídica |
| Conciliaciones | Conciliaciones Bancarias | Físico | Dirección de Recursos Físicos y Financieros |
| Contratos | Contrato de Adquisición de Bienes O Servicios | Físico y Electrónico | Secretaría General |
| Contratos | Contratos de Comodatos | Físico | Dirección de Recursos Físicos y Financieros |
| Contratos | Contrato de Prestación de Servicios | Físico y Electrónico | Secretaría General |
| Convenios | Convenio de Cooperación | Físico | Contraloría Auxiliar de Apoyo Técnico |
| Convenios | Convenio Interadministrativos | Físico | Contraloría Auxiliar de Apoyo Técnico |

**Fuente:** Registro de Activos de Información / página web www.cgm.gov.co; consulta realizada el 11/10/2021 – Sección Transparencia y Acceso a la Información Pública

Lo anterior, permite concluir que si bien se tienen identificados riesgos relacionados con pérdida de la confidencialidad, pérdida de integridad y pérdida de disponibilidad, se debe dar aplicación a la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5; en la cual se establece que "*para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso";* para a partir de allí establecer los demás elementos pertinentes a la metodología, entre otras la definición del nivel de criticidad partiendo de la criticidad respecto a la confidencialidad, la integridad y la disponibilidad del activo de los procesos.

Por lo anterior, no se continúa con la verificación de los demás pasos establecidos para la gestión de los riesgos relacionados con la Seguridad de la Información.

## 7.4 VALORACIÓN DEL RIESGO

De acuerdo con la guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de 2020, la estructura para el desarrollo de la valoración del riesgo, corresponde a la siguiente:

Figura 16. Estructura para la valoración de Riesgos


**Fuente:** Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de 2020.

Y de este paso, entre otras hacen parte el análisis del riesgo y la evaluación del riesgo; por lo que a continuación se hace una revisión de estas en la gestión de riesgos de la entidad.

### 7.4.1 Análisis de Riesgos

Conforme a la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de 2020, en el análisis del riesgo, "se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto"; y como parte de la *Evaluación del Riesgo,* que corresponde a un paso posterior, "*a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE)*"

A continuación se presenta lo evidenciado para algunos riesgos, durante las reuniones realizadas con las diferentes dependencias en relación con la probabilidad y el impacto; así como la Zona de Riesgo en que queda ubicado; así como el análisis realizado por la Oficina de Control Interno; veamos:

Tabla 9. Análisis de impacto y probabilidad de los Riesgos

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posibilidad de afectación reputacional, por incumplimiento de metas y objetivos, debido a la falta de seguimiento a las metas trazadas por parte de los líderes de los procesos. | 4 | **Baja** | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal | **Mayor** | **Alto** | En el caso de considerarse el riesgo relacionado con la posible pérdida de la certificación anual por parte de la AGR por incumplimiento de metas y objetivos, el impacto inherente afectaría la imagen de la Entidad a nivel nacional, con lo que el impacto del riesgo sería catastrófico, y se ubicaría en una zona de riesgo inherente extrema. |
| Posibilidad de afectación reputacional, por la desactualización del SIG, debido a la falta de seguimiento y revisión de los elementos del SIG por parte de los servidores de la entidad a fin de mantener el SIG actualizado. | 12 | **Baja** | El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores | **Menor** | **Moderado** | Es importante tener en cuenta que de acuerdo con la Guía para la Administración de Riesgos en Entidades Públicas versión 5, se establece que para definir el nivel de probabilidad "la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año", en el caso del riesgo identificado, se planteó para 12 meses, sin considerar lo establecido en la Guía, sin embargo, si se considera el riesgo cómo está definido, la actualización del SIG se puede realizar todos los días de la vigencia y teniendo en cuenta que para su gestión se utiliza un aplicativo, que puede presentar fallas en su funcionamiento.<br><br>Respecto al impacto definido, dado que no se plantea en términos de la posible pérdida de la certificación, no se estaría teniendo en |

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| | | | | | | cuenta que podría ser de conocimiento no solamente del ICONTEC, como ente de certificación, sino también de los diferentes grupos de interés de la Contraloría a nivel nacional, con lo que el impacto del riesgo sería catastrófico, y se ubicaría en una zona de riesgo inherente extrema. |
| Posibilidad de afectación económica y reputacional, por declaratoria de nulidad y/o imposición de la obligación de resarcir, debido a la elaboración de actos administrativos con fallas en la fundamentación fáctica y jurídica. | 40 | **Media** | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal | **Mayor** | **Alto** | De acuerdo a la reunión sostenida con los servidores de la Oficina Asesora Jurídica, se pudo evidenciar la aplicación de la metodología, entre otros, para la definición de la probabilidad, relacionada con la frecuencia de la actividad, así como con el impacto |
| Posibilidad de afectación económica y reputacional, por fallos judiciales con condenas patrimoniales en contra de la Entidad y de los sujetos de control, debido a la falta de verificación de términos procesales y judiciales. | 20 | **Baja** | Entre 10 y 50 SMLMV | **Menor** | **Moderado** | De acuerdo a la reunión sostenida con los servidores de la Oficina Asesora Jurídica, se pudo evidenciar la aplicación de la metodología, entre otros, para la definición de la probabilidad, relacionada con la frecuencia de la actividad, así como con el impacto; sin embargo, es importante revisar si efectivamente el impacto es menor, en caso de un fallo judicial en contra de la entidad, que podría afectar la reputación de la entidad con efecto a nivel nacional; lo que implicaría que el riesgo cambie de zona de riesgo inherente. |

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posibilidad de afectación reputacional, por el uso inadecuado de los medios y canales de comunicación, debido al desacato de las directrices y políticas emitidas por la Oficina Asesora de Comunicaciones de la entidad. | 730 | **Alta** | El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores | **Menor** | **Moderado** | Es importante evaluar si el impacto de una pérdida reputacional, puede ser considerada como menor, en especial teniendo en consideración que es un tema relacionado con la comunicación y que puede ser a nivel no sólo regional, sino también nacional; lo que implicaría que el riesgo cambie de zona de riesgo inherente. |
| Posibilidad de afectación reputacional, por la pérdida de información documentada, debido a omitir la entrega de los inventarios documentales, la no devolución de los documentos prestados o causas naturales. | 240 | **Media** | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos | **Moderado** | **Moderado** | En la revisión realizada con la dependencia se pudo establecer que para la definición de la frecuencia se consideró 240 días hábiles que en promedio tiene el año; sin embargo, en relación con la gestión documental, se tiene relacionado el uso del aplicativo Mercurio y que conforme a la guía " *"En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez*"; adicionalmente se podría presentar una posible sanción por incumplimiento de la Ley 594 de 2000 y esto podría ser de conocimiento nacional, lo que implicaría que el riesgo está considerado en una zona de riesgo inherente que no corresponde. |
| Posibilidad de afectación reputacional, por información documental no disponible para su acceso, debido a la Inaplicación de las Tablas de Retención Documental. | 240 | **Media** | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos | **Moderado** | **Moderado** | |

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posibilidad de afectación reputacional, por producir evaluaciones sin rigor técnico con resultados errados, quejas de las partes interesadas e investigaciones de entes reguladores y disciplinarios, debido a: Desconocimiento de los procesos, riesgos y normativa de la entidad auditada; debilidades en la planeación de auditorías en cuanto al alcance, conformación de equipos, tiempos, temas a auditar y perfil del equipo auditor; Inoportunidad, insuficiencia o mala calidad de la información rendida; deficiencias de control y supervisión en el desarrollo del proceso auditor; debilidades en la evaluación de los principios fiscales y en la formulación y soporte de los posibles hallazgos con incidencia fiscal; emisión de informes que contienen conclusiones y/o hallazgos que no concuerdan con la realidad de la gestión y resultados del sujeto de control. | 72 | **Media** | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal | **Mayor** | **Alto** | En el impacto, en caso de una investigación por auditorías sin rigor técnico, podría incluso tener un impacto a nivel nacional; lo que implicaría que el riesgo se encuentre en un nivel catastrófico y más aun teniendo en cuenta que esta actividad corresponde a su misión como entidad; por lo cual, con el cambio del impacto, la zona de riesgo inherente, pasaría de Alto a Extremo. |

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posibilidad de afectación económica y Reputacional por sanciones de los entes reguladores por presentación de información extemporánea o incompleta de estados financieros con salvedades, debido a fallas en la aplicación de los controles establecidos en la gestión financiera para el cierre | 240 | **Media** | Afectación menor a 10 SMLMV. | **Leve** | **Moderado** | Es importante tener en cuenta que de acuerdo con la Guía para la Administración de Riesgos en Entidades Públicas versión 5, se establece que para definir el nivel de probabilidad "la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año", en el caso del riesgo identificado, se planteó para 240 días hábiles, sin considerar lo establecido en la Guía, siendo importante tener en cuenta que el riesgo está relacionado con la presentación extemporánea o incompleta de estados financieros.<br>Respecto al criterio de impacto definido, durante la reunión sostenida con los servidores de la Dirección de Recursos Físicos y Financieros, no fue posible identificar la fuente para determinar la posible afectación económica, por lo cual es importante que de acuerdo al riesgo se identifique por quien puede ser sancionado económicamente la Contraloría y el monto máximo al cual se podía ver expuesta, y el posible impacto reputacional debido a la afectación de la imagen de la Entidad frente a los grupos de interés; conllevando a que el riesgo pueda estar en una zona de calor diferente. |

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posibilidad de afectación económica y reputacional, por Sanción del ente regulador por interpretación inadecuada o incumplimiento de la norma y desaprovechamiento de los recursos financieros, debido a fallas en la aplicación de los controles en la ejecución presupuestal | 4 | **Baja** | Entre 50 y 100 SMLMV | **Moderado** | **Moderado** | Respecto a la frecuencia con la cual se realiza la actividad, en la reunión sostenida con los servidores de la Dirección de Recursos Físicos se pudo evidenciar que la misma corresponde a 4 seguimientos trimestrales, sin embargo, se debe tener en cuenta lo establecido en la Guía para la Administración de Riesgos, numeral 3.1.1. en la que se establece que "la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año", por lo que es importante determinar con claridad la frecuencia con la que se lleva a cabo la actividad, conforme a la Guía. Lo anterior implicaría que la ubicación del riesgo inherente en la zona de calor sea diferente.<br>Respecto al criterio de impacto definido, durante la reunión sostenida con los servidores de la Dirección de Recursos Físicos y Financieros, no fue posible identificar la fuente para determinar la posible afectación económica, por lo cual es importante que de acuerdo al riesgo se identifique por quien puede ser sancionado económicamente la Contraloría y el monto máximo al cual se podía ver expuesta; conllevando a que el riesgo pueda estar en una zona de calor diferente. |

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posibilidad de afectación económica por bienes muebles sin amparo en pólizas de seguros, debido a omisión en el reporte de bienes muebles adquiridos, para ser incluidos en la póliza de seguros | 12 | **Baja** | Entre 10 y 50 SMLMV | **Menor** | **Moderado** | Para la definición de la probabilidad, se estableció para 12 meses, sin considerar que el riesgo está relacionado actualmente con la "...omisión en el reporte de bienes muebles adquiridos, para ser incluidos en la póliza de seguros".<br>Respecto al criterio de impacto definido, durante la reunión sostenida con los servidores de la Dirección de Recursos Físicos y Financieros, no fue posible identificar la fuente para determinar la posible afectación económica, por lo cual es importante que de acuerdo al riesgo se identifique el monto máximo y posibles afectaciones a la imagen, a las cuales se podía ver expuesta la Entidad; conllevando a que el riesgo pueda estar en una zona de riesgo inherente diferente. |

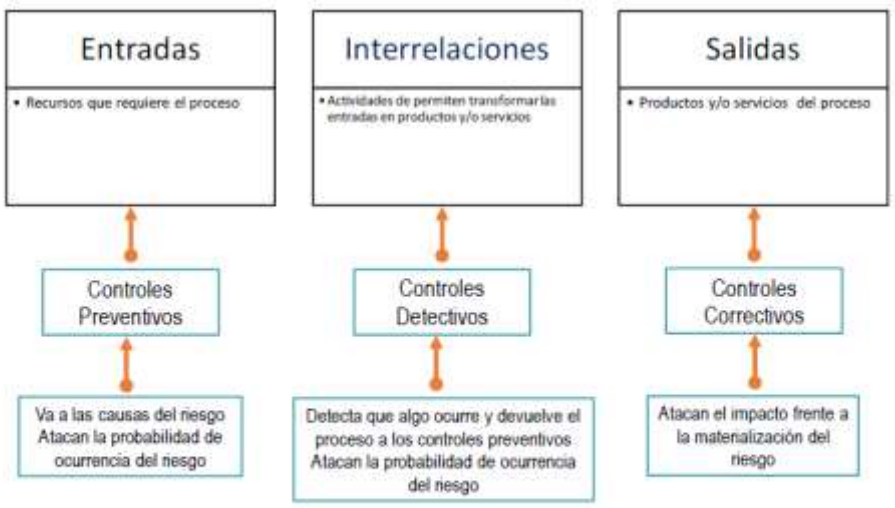
| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posibilidad de afectación reputacional, por reclamaciones de los servidores públicos por la nómina, debido a la Inconsistencia en la liquidación de la bonificación por servicios prestados en el sistema de nómina. | 24 | **Baja** | El riesgo afecta la imagen de alguna área de la organización | **Leve** | **Bajo** | Para la definición de la probabilidad se consideró el total de nóminas liquidadas durante la vigencia; sin embargo, no se tiene en cuenta que para su gestión se dispone de un aplicativo que puede presentar inconsistencias y que conforme a la guía, "*En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez*" Adicionalmente se indica que impacta solamente la imagen de un área; sin embargo, por inconsistencias en la liquidación de la nómina, se pueden generar inconsistencias en las retenciones y posteriores pagos a la DIAN, lo que podría implicar sanciones por parte de dicho ente; lo que implicaría que la zona de impacto pueda ser mayor y por ende la zona de riesgo inherente puedan cambiar a Alta; sin tener en cuenta la probabilidad. |
| Posibilidad de afectación económica y reputacional, por Sanciones de los entes reguladores por Inadecuada vinculación y desvinculación de los servidores públicos, debido a Fallas en la aplicación de los controles en el procedimiento para el ingreso y retiro | 30 | **Media** | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos | **Moderado** | **Moderado** | En relación con el impacto, no se consideró que las posibles "*Sanciones de los entes reguladores por Inadecuada vinculación y desvinculación de los servidores públicos…*", podría afectar la imagen de la Entidad a nivel municipal e incluso nacional; por lo que el impacto podría ser mayor, incluso catastrófico, que conllevaría que el riesgo se encuentre en una zona alta o extrema. |

| Descripción del Riesgo | Frecuencia con la cual se realiza la actividad | Probabilidad Inherente | Criterios de impacto | Impacto Inherente | Zona de Riesgo Inherente | Observaciones OCI |
|---|---|---|---|---|---|---|
| Posible pérdida reputacional y económica por sanciones, procesos disciplinarios y disminución de la certificación anual de gestión de la Contraloría, debido a la inoportunidad en la rendición de la cuenta y que ésta no sea de calidad, consistente, coherente, y veraz. | 550 | **Alta** | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal | **Mayor** | **Alto** | En relación con este riesgo, la posible disminución de la certificación anual de gestión de la Contraloría, podría implicar la posible intervención administrativa por parte de la Contraloría General de la República, debido a que el índice AuditeCT para la contraloría, sea menor al puntaje crítico de certificación anual, conforme a la metodología definida por la AGR; lo que implicaría que el impacto pueda ser a nivel nacional, quedando en un nivel de impacto catastrófico y por ende en una zona de riesgo inherente extrema. |

### 7.4.2 Evaluación del Riesgo

Para realizar la evaluación del riesgo, es importante tener en cuenta la tipología de los controles; conforme a lo establecido en la guía y que en términos generales se clasifican en Controles Preventivos, Controles Detectivos y Controles Correctivos; veamos:

Figura 17. Tipología de los Controles



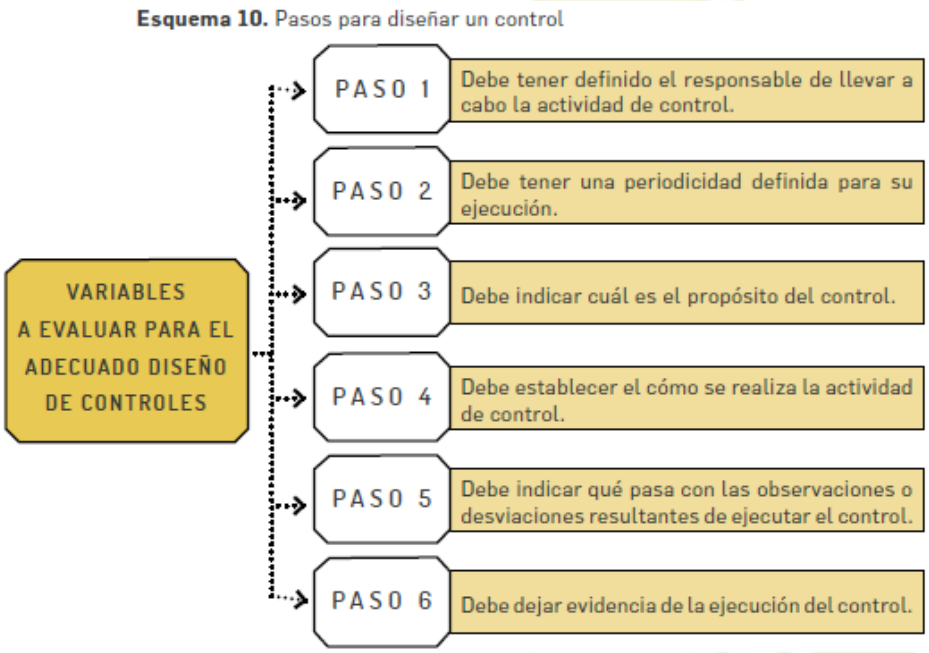

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**Fuente:** Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de 2020.

En relación con los riesgos de gestión, se evidenciaron un total de 52 controles; de los cuales 32 fueron clasificados como preventivos, 17 como Detectivos y 3 como correctivos.

Adicionalmente, al momento de realizar el diseño de los controles, la guía establece lo siguiente: ""*Tenga en cuenta para el diseño de controles, los parámetros señalados en la* ***versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes****, por lo tanto se sugiere remitirse a dicho documento*" y conforme a la guía los pasos son los siguientes:

Figura 18. Esquema para el diseño de controles




**Fuente:** Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de 2020.

A continuación se presenta un análisis de los controles diseñados para los riesgos de gestión identificados; veamos:

Tabla 10. Análisis de las actividades de control definidas

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| Posibilidad de afectación reputacional, por incumplimiento de metas y objetivos, debido a la falta de seguimiento a las metas trazadas por parte de los líderes de los procesos. | 1 | El profesional de la OA de Planeación, trimestralmente revisa el avance o cumplimiento de las metas, mediante la consolidación del seguimiento del plan de acción. En caso de identificar un posible incumplimiento de las metas, realizará mediante correo electrónico solicitud al líder responsable del proceso, para que defina y ponga en marcha las acciones que garanticen el cumplimiento de las metas propuestas.<br>Evidencia: Seguimiento trimestral al Plan de Acción y Correos electrónicos. | Al evaluar los atributos se indica que el control es preventivo; sin embargo, con el mismo se evidencia si están cumpliendo o no las metas y objetivos; por lo cual, el control es detectivo; por lo que la calificación disminuiría a 30%.<br><br>Con respecto a la documentación, la Guía de Evaluación del Desempeño Institucional, Código G-GES-ED-001, versión 1, plantea que "*se identifica como puntos de control la actividad 3 y 6, para el cumplimiento de los requisitos*", que corresponden a que se *"...envía recordatorios a los directivos, para que remitan los seguimientos a la Oficina Asesora de Planeación...*" y que se "*...revisa el seguimiento y solicita los ajustes pertinentes si es del caso...*"; sin embargo, se evidencia entre las actividades definidas que se "...presenta el seguimiento al Plan de Acción Institucional como entrada para la revisión por la Dirección ante el Consejo de Dirección..."; por lo que sólo se evidencia registrado uno de los controles en la matriz de riesgos.<br><br>Adicionalmente no se evidencia segregación frente a los controles definidos en el mapa de riesgos.<br><br>Los demás atributos del control están conformes a la guía. |
| Posibilidad de afectación reputacional, por la desactualización del SIG, debido a la falta de seguimiento y revisión de los elementos del SIG por parte de los servidores de la entidad a fin de mantener el SIG actualizado. | 1 | El profesional Universitario y el técnico Operativo de la Oficina Asesora de Planeación, permanentemente validará las solicitudes de ajustes documentales del SIG solicitada por las dependencias, registrando el control en la naturaleza de cambios y en el archivo Excel "Registro de actividades al SIG". Caso tal que se identifique que la solicitud presente inconsistencias, se devuelve al responsable para su revisión o aclaración. | El control definido corresponde a una actividad, y con este no se atacan las causas de fondo de la posible desactualización del SIG, que se puede deber a los cambios normativos que afectan los procesos y si se tiene en cuenta la posible pérdida de la certificación por parte del Icontec, este se podría deber, adicional a lo anterior, a la falta de implementación, mantenimiento y mejoramiento del SIG, entre otras por la rotación del personal directivo, toda vez que conforme a la política de información documentada del Manual de Políticas de operación, se establece que: "Los líderes de proceso deben revisar periódicamente los documentos dispuestos |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| | | Evidencia: Archivo Excel - Registro de actividades al SIG.<br>Correo electrónico. | en el aplicativo Isolución, y enviar los ajustes o modificaciones por Mercurio o correo electrónico a la Oficina Asesora de Planeación...".<br><br>Adicionalmente, para la actualización del SIG, no se dispone de un plan de trabajo anual donde se establezcan periódicamente las revisiones a la documentación de los procesos, y que conforme al Acuerdo 087 de 2018 se establece como funciones de la Oficina Asesora de Planeación, la de "identificar, proponer y planificar los cambios en el Sistema Integral de Gestión" y para el Comité Institucional de Coordinación de Control Interno, según Resolución 604 de 2020, artículo 4, literal 1, le corresponde "...*aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del sistema de control interno a partir de la normativa vigente...*".<br><br>El control definido no es de carácter preventivo, dado que no evita que el sistema esté desactualizado, adicionalmente, en la Guía denominada "Información Documentada", es importante precisar las gestiones que se realizan a través de la Secretaría General, la Oficina Asesora de Planeación y el CICCI, frente a la elaboración, revisión y la aprobación de documentos relacionados con el SIG.<br><br>Es importante tener en cuenta los lineamientos establecidos en la Guía de la función pública, para la definición de los controles, entre otras, porque no se diferencia la actuación del profesional universitario y del técnico operativo.<br><br>Los demás atributos del control están conformes a la guía. |
| | 2 | El profesional Universitario y técnico Operativo de la Oficina Asesora de Planeación, al iniciar la vigencia verificará en el registro de actividades al SIG, la documentación que no ha registrado actualización durante la misma, mediante la revisión de las fechas. En caso de evidenciar documentos sin actualización validamos previa información de la dependencia la necesidad o no de la actualización.<br>Evidencia: Correo electrónico. Archivo Excel - Registro de actividades al SIG actualizado por fechas. | |
| Posibilidad de afectación económica y reputacional, por declaratoria de nulidad y/o imposición de la obligación de resarcir, debido a la elaboración de actos administrativos con | 1 | El Jefe de la Oficina Asesora Jurídica o el Contralor, revisa los proyectos de acto administrativo (responsabilidad fiscal, disciplinarios, etc.) con el fin de validar si tiene la adecuada fundamentación fáctica y jurídica. En caso de requerir ajuste lo devolverá al profesional con las observaciones pertinentes. Se deja evidencia en los mismos actos administrativos | Verificado el procedimiento denominado "gestión Jurídica" versión 10, se evidenció el siguiente control, relacionado, entre otros, con los proyectos de acto administrativo: "*revisar y dar visto bueno al proyecto acto administrativo. Enviarlo al Contralor para lo de su competencia*", cuyos responsables figuran el Jefe de la Oficina Asesora Jurídica y el Profesional Universitario, sin que se evidencie la gestión del Contralor en la aplicación de dicho control; adicionalmente se tiene |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| fallas en la fundamentación fáctica y jurídica. | | por medio del visto bueno, el correo o en un comentario de Mercurio. | establecido "*Verificar cumplimiento y realizar seguimiento a la ejecución de términos legales y la oportunidad en la expedición de actos administrativos...*"<br>Para la definición del control, es importante que se dé cumplimiento a lo establecido en la Guía, en especial lo relacionado con el numeral 3.2.2.1 Estructura para la descripción del control, y separar las actividades realizadas tanto por la Jefe de la Oficina Asesora Jurídica, la Contralora y el Profesional Universitario que permitan evidenciar la segregación de funciones.<br>El control definido corresponde a un control detectivo, toda vez que el mismo se ejecuta durante las interacciones del proceso, previo a la aprobación del acto administrativo; por lo que la calificación del control pasaría a 30%.<br>Los demás atributos del control están conformes a la guía. |
| Posibilidad de afectación económica y reputacional, por fallos judiciales con condenas patrimoniales en contra de la Entidad y de los sujetos de control, debido a la falta de verificación de términos procesales y judiciales. | 1 | El profesional asignado para el caso, cada vez que se recepcione un requerimiento por parte de un Despacho judicial, con el fin de establecer la fecha máxima de intervención en el proceso. Formato Registro de Actividades de Servidores Públicos, que se le presenta mensualmente al jefe. | La redacción contenida en la descripción del control, no permite establecer el control que se va a ejecutar, incumpliendo lo establecido en la guía para la administración de riesgos.<br>No se cumplen los atributos del control establecidos en la guía. |
| Posibilidad de afectación reputacional, por el uso inadecuado de los medios y canales de comunicación, debido al desacato de las directrices y políticas emitidas por la Oficina Asesora de Comunicaciones de la entidad. | 1 | El equipo de servidores públicos de la OA de Comunicaciones previo a la emisión de mensajes, verificará que cumplan las directrices y políticas emitidas por la O A de Comunicaciones de la entidad, cotejando con los requisitos establecidos para cada una de las piezas comunicacionales. La evidencia de la aplicación del control se consignará en los grupos primarios. | El control establecido no es claro, no se evidenció registrado en el Procedimiento de Comunicación Pública; adicionalmente aunque se indica que es continuo, en la redacción indica lo contrario, toda vez que establece que " La evidencia de la aplicación del control se consignará en los grupos primarios"; no siendo oportuna su aplicación. |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| Posibilidad de afectación reputacional, por la pérdida de información documentada, debido a omitir la entrega de los inventarios documentales, la no devolución de los documentos prestados o causas naturales. | 1 | El técnico operativo anualmente verifica el diligenciamiento del Formato Único de Inventario Documental, entregados por las dependencias, en el caso de encontrar inconsistencias, solicita los respectivos ajustes a los responsables de los Archivos de Gestión.<br>Evidencia: FUID, Transferencia Primaria | El control relacionado con "...seguimiento a los préstamos de documentos", es detectivo y no preventivo como se estableció.<br>En los controles definidos no se observa segregación de funciones; quedando toda la responsabilidad en el Técnico Operativo.<br>Adicionalmente, en relación con la posible pérdida de información documentada, no se tiene en cuenta los inconvenientes que se puedan presentar con el aplicativo Mercurio, el cual es utilizado para la conservación documental y por lo tanto no se identificaron controles. |
| | 2 | El técnico Operativo mensualmente realiza el seguimiento a los préstamos de documentos, registrados en el control de consultas y préstamos, en caso de identificar la no devolución del documento o renovación del préstamo, se realiza el requerimiento al usuario.<br>Evidencia: Planilla y correo electrónico | |
| | 3 | El técnico operativo trimestralmente verificará que se cuente con elementos de seguridad Industrial y sus certificaciones, en caso de que se detecte equipos que no cumplan con las condiciones requeridas, solicitará a la Dirección de Talento Humano, el mantenimiento o actualización de los mismos.<br>Evidencia: Informe Archivo Central y Correo electrónico | |
| Posibilidad de afectación reputacional, por producir evaluaciones sin rigor técnico con resultados errados, quejas de las partes interesadas e investigaciones de entes reguladores y disciplinarios, debido a: | 1 | La Subcontraloría y el Contralor Auxiliar, verifican previamente la disponibilidad de los recursos necesarios para la programación de las Auditorias del plan de vigilancia y control Fiscal (tiempo, temas, talento humano con perfiles adecuados entre otros); en caso de requerir apoyo técnico y/o de un experto, se harán las gestiones necesarias. Labor que se hará antes de asignar cada Auditoría.<br>Evidencia: PVCFT-CGM, memorando de asignación, Solicitud de apoyo y respuesta | Con respecto al primer control, no se indica la evidencia que se genera; sin embargo, conforme a la documentación del proceso, se dispone del Papel de Trabajo PT 02 PF-Gestión del Riesgo de Auditoría, que se debe diligenciar y en el que entre otras se evalúa la experticia, el conocimiento, la formación y la comprensión de la auditoría. No cumple con todos los atributos del control.<br><br>En el segundo control se tiene 2 controles diferentes; sin embargo, el que se realiza por parte del Supervisor, no cumple con todos los atributos del control; así mismo, en lo que respecta al control que ejecuta el Equipo Auditor, no es preventivo, sino detectivo. |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| Desconocimiento de los procesos, riesgos y normativa de la entidad auditada; debilidades en la planeación de auditorías en cuanto al alcance, conformación de equipos, tiempos, temas a auditar y perfil del equipo auditor; Inoportunidad, insuficiencia o mala calidad de la información rendida; deficiencias de control y supervisión en el desarrollo del proceso auditor; debilidades en la evaluación de los principios fiscales y en la formulación y soporte de los posibles hallazgos con incidencia fiscal; emisión de informes que contienen conclusiones y/o hallazgos que no concuerdan con la realidad de la gestión y resultados del sujeto de control. | 2 | El Supervisor (Contralor Auxiliar), en el desarrollo de la Auditoría, verifica que las solicitudes de información se hagan de manera oportuna, clara y suficiente. El Equipo Auditor revisa que las respuestas sean oportunas, suficientes y de calidad, dejando evidencia en sus papeles de trabajo. En caso de que la respuesta no cumpla estas condiciones, se vuelve a requerir dando términos perentorios. Si no cumple se traslada a proceso sancionatorio. Esta labor se hará cada vez que se requiera. Evidencia: Oficios de requerimiento de información, respuestas, anotaciones en los papeles de trabajo y formato de traslado sancionatorio de ser el caso | Y con respecto al cuarto control, en este no se detallan las acciones a seguir en caso de que se evidencie incumplimiento.<br><br>Sin embargo, este riesgo reúne demasiados elementos que siendo considerados de manera independiente, deberían definir controles específicos para evitar su materialización.<br><br>Es importante tener en cuenta el control establecido en la Guía de Liberación de Productos y Control de Salidas No Conformes, Código:G-GES-LPC-001, Versión 4, en la que se establece que: "*La Liberación aplica para los productos definidos en la entidad en temas misionales y el control de salidas no conformes aplica para todas las salidas de los procesos…*"<br><br>Se eliminaron de este consolidado los controles 3, 5 y 6; toda vez que no se tenían comentarios al respecto. |
| | 4 | El supervisor (Contralor Auxiliar) y el Líder de Equipo de Auditoría, en la fase de ejecución de la auditoría, en mesa de trabajo, verifican la suficiencia, pertinencia y conducencia de las pruebas, mediante la revisión de los papeles de trabajo que soportan los resultados; verifican que se realicen las pruebas con la respectiva recopilación de evidencias acorde con lo establecido en el Plan de Trabajo y Programa de Auditoría. Esta labor se debe realizar al menos 2 veces en la etapa de ejecución (e) para garantizará la adecuada construcción de hallazgos y conclusiones del informe. Evidencia: Acta o Ayuda de memoria, papeles de trabajo | |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| Posibilidad de afectación económica y reputacional; por caducidad de la acción fiscal en los hallazgos fiscales, en las indagaciones preliminares que procedan de las denuncias ciudadanas y del traslado de otras entidades; debido a la inactividad procesal para calificar las los Hallazgos Fiscales y las Indagaciones Preliminares e iniciar los procesos de responsabilidad fiscal. | 1 | El Contralor Auxiliar de Responsabilidad Fiscal y Jurisdicción Coactiva con el apoyo del técnico operativo, verificará el recibo de los hallazgos y sus documentos equivalentes para su reparto, en un término de 8 días hábiles a partir del recibo de estos y comisionará mediante auto a los abogados sustanciadores. Evidencia: auto comisorio. | En estos controles, no se detalla la responsabilidad del Contralor Auxiliar de Responsabilidad Fiscal y Jurisdicción Coactiva y del Técnico Operativo, por lo que no se evidencia segregación de funciones; adicionalmente los controles son detectivos y no preventivos como fueron calificados.<br>Con respecto al primer control no se detalla la evidencia específica de la verificación de los hallazgos. Adicionalmente, no se indica que se debe hacer en caso de que se incumpla.<br>Los controles no cumplen con la totalidad de atributos definidos en la guía. |
| | 2 | El Contralor Auxiliar de Responsabilidad Fiscal y Jurisdicción Coactiva con el apoyo del técnico operativo, Revisará mensualmente en grupo primario el término de caducidad de los hechos en las Indagaciones preliminares que se encuentren aperturadas, En el caso que en la etapa de investigación en la Indagación Preliminar se detecten hechos caducados el abogado comisionado deberá realizar el archivo de los antecedentes. Evidencia: cuadro control de caducidad de indagaciones preliminares y el auto de archivo de antecedentes caducados que se realicen. | |
| Posibilidad de afectación reputacional, por la inadecuada e inoportuna respuesta a de las PQRSD a los ciudadanos, debido a la inaplicabilidad del Manual de Tramites de las PQRSD. | 1 | El técnico Operativo de la C.A Participación Ciudadana, verificara el diligenciamiento del formato de archivo de la PQRSD en lo correspondiente al requisito de fondo (Cumplir con los términos de Ley), forma (Dar respuesta en los formatos establecidos en el Workflow), en caso de detectarse el incumplimiento de alguno de estos, se le notificará al jefe de la dependencia para que realice nuevamente el diligenciamiento del formato y tenga en cuenta el campo de liberación con salvedad. Evidencia formato de archivo de la PQRSD. | En los controles definidos, no se evidencia segregación de funciones, ni los controles definidos para los líderes de procesos que tienen competencia en la gestión de las PQRSD; entre otras, para garantizar que se cumpla lo establecido en la norma cuando una PQRSD sea relacionada con una denuncia que deba ser resuelta a través del proceso auditor; así como que la respuesta sea de fondo y de forma; sin embargo, en el Manual Trámite Interno de PQRSD, Código: M-PC-TI-001, versión 3, se establece el siguiente control: "*El jefe de la dependencia verifica que la respuesta a la petición cumpla con los criterios de forma y fondo definidos en la caracterización del proceso como son: (Forma: Cumplir los requisitos de las comunicaciones oficiales externas y Fondo: Dar respuesta* |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| | 2 | El técnico operativo de la C.A Participación Ciudadana, clasifica el tipo de petición, valida los términos y genera las alarmas respectivas en mercurio para que le informe al servidor el avance de los términos para dar respuesta oportuna a las PQRSD. | *adecuado según la solicitud y Cumplir con los términos de Ley), firmar y enviar al secretario de su dependencia, para dar continuidad a la ruta del Workflow.*<br>*Si no cumple con los criterios definidos devolver para su corrección al servidor público que proyecto la respuesta*" y en este caso el control es detectivo.<br><br>El segundo y tercer control, son de carácter detectivo y no preventivo como se plantea, lo que implica que su calificación se disminuya a 30%.<br><br>Los controles definidos no cumplen con la totalidad de atributos definidos en la guía, entre otras, que se debe hacer en caso de incumplimiento. |
| | 3 | El técnico Operativo de la C.A Participación Ciudadana semanalmente realizara un reporte de las PQRSD que se encuentran en proceso y se vencen en la semana siguiente.<br>En caso de no tenerse PQRSD a vencer en la próxima semana no se envía reporte. | |
| Posibilidad de afectación económica y Reputacional por sanciones de los entes reguladores por presentación de información extemporánea o incompleta de estados financieros con salvedades, debido a fallas en la aplicación de los controles establecidos en la gestión financiera para el cierre | 1 | El Director Administrativo mensualmente, a partir del segundo semestre, envía memorando a las dependencias ejecutoras del presupuesto en el cual se indicará la importancia de la revisión del Plan Anual de Adquisiciones de acuerdo al porcentaje de ejecución presupuestal, así mismo, se hará referencia a los plazos que se estiman para el cierre y estos de acuerdo a los tiempos contractuales, también solicitar a la Oficina Asesora de Comunicaciones durante el cuarto trimestre, realizar recordatorios a las dependencias ejecutoras del presupuesto a través de los canales institucionales, sobre los compromisos establecidos en el cronograma de cierre financiero. | En relación con el primer control definido, es importante que se dé cumplimiento a lo establecido en la Guía, en especial lo relacionado con el numeral 3.2.2.1 Estructura para la descripción del control, toda vez que el control definido corresponde a una actividad.<br><br>Respecto al segundo control, dado que su ejecución es anual, este control no es oportuno, toda vez que la presentación de información extemporánea no solamente se genera al finalizar la vigencia; sin embargo, a través de las evaluaciones independientes realizadas por la Oficina de Control Interno, se han evidenciado controles mensuales para los respectivos cierres, que no se encuentran actualmente documentados. |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| | 2 | El Director Administrativo de Recursos Físicos y Financieros, anualmente, verifica el cumplimiento en la entrega de información para conciliar y ajustar la información financiera, mediante la revisión de los tiempos establecidos en el cronograma y llevando el control en hoja de Excel, de la entrega de la información por parte de las dependencias. En caso de requerir ajustes o presentarse incumplimientos en el envío de la información se solicita al área que incumple. | Adicionalmente, es importante considerar la existencia de otras posibles causas y con ello controles adicionales relacionados con la posibilidad de presentación extemporánea de información financiera o imprecisa, entre otros, a la AGR, a la Contaduría General de la Nación o la DIAN, en cuyo caso se podrán generar sanciones a la entidad. |
| | 3 | El profesional universitario (Contador), diariamente verifica el registro contable mediante la revisión de la causación de las retenciones, soportes, valores, cotejo con proveedores y terceros, cuentas inconsistentes y de encontrarse consistente con los requisitos, firma la causación y pasa a Tesorería para continuar el trámite. En caso de encontrar observaciones en el registro contable, devuelve los documentos físicos para la corrección y registra en el sistema reversión de la operación. | |
| Posibilidad de afectación económica y reputacional, por Sanción del ente regulador por interpretación inadecuada o incumplimiento de la norma y desaprovechamiento de los recursos financieros, | 1 | El servidor público responsable del manejo presupuestal verificará el cumplimiento de la normativa en la ejecución del presupuesto confrontando las disposiciones normativas (Decreto de liquidación del presupuesto) con las necesidades definidas en los estudios previos, además en caso de presentarse una duda en la interpretación de la norma se solicitará concepto a la instancia competente. | Verificado el procedimiento de Presupuesto versión 9, se evidenció, entre otros, el siguiente control: "*Revisar que todas las operaciones para el cierre anual del presupuesto cumpla con todo lo estipulado en las normas vigentes*", el cual es ejecutado por el Director Administrativo de Recursos Físicos y Financieros y del que queda acta de mesa de trabajo, siendo importante incluir dicho control en la matriz de riesgos del proceso previo la revisión de la viabilidad de su ejecución (conforme está definido). |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| debido a fallas en la aplicación de los controles en la ejecución presupuestal | 2 | El Director Administrativo de Recursos Físicos y Financieros, trimestralmente presentará ante el Comité Financiero el seguimiento a la ejecución presupuestal, con el fin de que se tomen las decisiones oportunas y pertinentes. En caso de encontrar rubros con déficit se solicita el traslado ante el Municipio de Medellín.<br>Evidencia reporte ejecución presupuestal, archivo Excel papel de trabajo, acta Comité Financiero. | Respecto al primer control no se encontró documentado en el procedimiento, así mismo, no se identifica la evidencia que queda una vez se ejecuta el control; por lo cual, para la definición del control, es importante que se dé cumplimiento a lo establecido en la Guía, en especial lo relacionado con el numeral 3.2.2.1 Estructura para la descripción del control, respecto a la definición de la acción a realizar y la evidencia que se genera. |
| Posibilidad de afectación económica por bienes muebles sin amparo en pólizas de seguros, debido a omisión en el reporte de bienes muebles adquiridos, para ser incluidos en la póliza de seguros | 1 | El técnico operativo verifica que la totalidad de bienes adquiridos hayan sido reportados a la aseguradora, confrontando en un archivo de Excel que cada bien adquirido tenga asociado el número del radicado del oficio remisorio al municipio de Medellín, para su aseguramiento, en caso de identificar algún activo sin radicado asociado se reportará a la aseguradora.<br>Evidencia: papel de trabajo en Excel | Verificado el procedimiento de Administración y Mantenimiento de Bienes muebles e inmuebles versión 3, no se evidenció el control definido, adicionalmente, conforme a lo establecido en la Guía de Administración de Activos fijos versión 2, entre los mecanismos de prevención de riesgos en el manejo de los activos fijos, se encuentra "...la revisión periódica de los bienes en cartera" y "...la revisión periódica para incluir en el análisis, nuevos bienes o recursos desprotegidos", los cuales consideramos corresponden a la conciliación que se puede hacer entre el universo (totalidad de bienes susceptibles de asegurar en la Entidad) frente a la relación de bienes asegurados reportados por la aseguradora. |

| Descripción del Riesgo | No. Control | Descripción del Control | Observaciones OCI |
|---|---|---|---|
| Posibilidad de afectación reputacional, por reclamaciones de los servidores públicos por la nómina, debido a la Inconsistencia en la liquidación de la bonificación por servicios prestados en el sistema de nómina. | 1 | Los técnicos operativos quincenalmente, verifican la correcta liquidación de nómina y prestaciones sociales, revisando los resultados vs las novedades y situaciones ingresadas y posteriormente realizan revisión de toda la nómina en forma manual. En caso de encontrar inconsistencia se corrige la novedad y se reliquida la nómina, evidencia registro de las novedades de nómina y prestaciones sociales reportados en los expedientes correspondientes. Evidencia: Papel de trabajo | Con respecto al control definido, el mismo es de carácter detectivo y no preventivo como se tiene asignado.<br><br>Verificado el procedimiento denominado "Liquidación de Nómina, Prestaciones Sociales, Cesantías Parciales y Definitivas" versión 10, se evidenciaron, entre otros, los siguientes controles: "*Confrontar y verificar listado de inconsistencias que arroja el sistema kactus, realizar las pruebas necesarias en hojas electrónicas, y verificar ajustes y correcciones de todas las novedades e incapacidades reportadas*", cuyos responsables figuran el Técnico Operativo y el Profesional Universitario, sin que se detalle cual es el registro que se genera con la ejecución de estos controles.<br><br>Para la definición del control, es importante que se dé cumplimiento a lo establecido en la Guía, en especial lo relacionado con el numeral 3.2.2.1 Estructura para la descripción del control, y separar las actividades realizadas tanto por el Técnico Operativo como por el Profesional Universitario que permitan evidenciar la segregación de funciones. |
| Posibilidad de afectación Económica y reputacional, por reclamaciones de los servidores públicos y las entidades prestadoras de salud, Fondo de Pensiones y Cesantías; debido a la Inconsistencia en la liquidación de la Seguridad Social. | 1 | El Profesional Universitario mensualmente, verifican la correcta liquidación de la seguridad social, revisando los valores del archivo que se extrae de Kactus vs las novedades que se presentan en el mes a cotizar. En caso de encontrar inconsistencia se corrige y se reliquida nuevamente, una vez verificada que las correcciones se encuentren realizadas se procede al cargue en la plataforma de Arus. Evidencia Papel de trabajo Seguridad Social. | Se evidenció en el procedimiento de liquidación de Nómina, Prestaciones Sociales, Cesantías Parciales y Definitivas versión 10, el control "Verificar que se hayan tenido en cuenta las novedades e incapacidades reportadas", cuyos responsables figuran el Técnico Operativo y el Profesional Universitario, sin que se detalle cual es el registro que se genera con la ejecución de estos controles.<br><br>Comparado el control definido en el procedimiento y el contenido en el mapa de riesgos, se evidenció en la reunión realizada con la Profesional Universitaria 1 de la Dirección de Talento Humano, responsable del tema, que el control que se aplica es el control definido en la matriz de riesgos y del cual se tiene evidencia de su ejecución.<br>El control definido corresponde a un control detectivo, toda vez que el mismo se ejecuta durante las interacciones del proceso, previo al pago de la Nómina. |

De la revisión realizada, se pudo evidenciar, entre otras lo siguiente:

- Existen controles que se encuentran definidos en las diferentes políticas de operación, que no fueron tenidos en cuenta al momento de analizar los controles relacionados con el riesgo.

- Se debe garantizar el cumplimiento de la metodología al momento de definir los diseñar los controles

- Dado que los controles correctivos, permiten disminuir el impacto de los riesgos; es importante profundizar en los posibles controles para los riesgos pertinentes en la entidad.

- Es importante tener en cuenta el control establecido en la Guía de Liberación de Productos y Control de Salidas No Conformes, Código: G-GES-LPC-001, Versión 4, en la que se establece que: "*La Liberación aplica para los productos definidos en la entidad en temas misionales y el control de salidas no conformes aplica para todas las salidas de los procesos…*", en especial, porqué en ella se establecen las acciones a seguir cuando se evidencia una salida no conforme.

- Entre las estrategias definidas para combatir el riesgo, se encuentra el trasferir, en el que "*después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas*" y en ninguno de los casos se evidenció la transferencia del riesgo.

## 7.5 MONITOREO Y REVISIÓN DE LOS RIESGOS

De conformidad con la Política de Administración del Riesgos, que se encuentra incluida en el Manual de Políticas de Operación, Código: M-GE-PL-002, Versión 7; "*Se realizará trimestralmente por parte de la primera línea de defensa y sus equipos de trabajo en los grupos primarios, quienes deberán registrar en el aplicativo Isolución, el seguimiento a la aplicación de cada uno de los controles definidos y de las acciones que según la metodología se hayan establecido para reducir el riesgo en las respectivas acciones para abordar los riesgos",* en cumplimiento de lo anterior, se verificó en el aplicativo Isolución / módulo de mejora y se evidenció registradas las acciones para abordar los riesgos, con su respectivo seguimiento, por parte de la Primera Línea de Defensa.

Una vez analizados los seguimientos realizados de manera trimestral, se pudo evidenciar lo siguiente:

- Se evidenció en la guía de evaluación del desempeño institucional y en las directrices del seguimiento al PAI, las directrices para realizar el seguimiento; sin embargo, en un alto número de acciones para abordar los riesgos, el seguimiento que se realiza es el mismo cada trimestre; sólo se cambian algunos datos.

- Los seguimientos que se realizan, en algunos casos son iguales a la actividad que se plantea.

- En el seguimiento que se realiza a algunas acciones para abordar los riesgos, se indica que no se ha materializado el riesgo; sin embargo en la Política de Administración de Riesgos no se dan lineamientos frente a las gestiones que se deben adelantar en caso de materialización de los riesgos; solamente se plantea para los procesos contractuales, que "*la Secretaria General consolidará estos resultados y la posible materialización de algún riesgo, de lo cual presentará informe ante el Consejo de Dirección*".

  Conforme al memorando 202100009800 del 17/11/2021, de la Oficina Asesora de Planeación, al respecto se plantea que: "*En las directrices para el seguimiento del PAI, se establece que en caso de que se hay materializado un riesgo debe notificar de manera inmediata a la OAP, para dar las indicaciones a seguir, y en la guía de evaluación del desempeño esta descrito lo siguiente: "Para el monitoreo deberá tener en cuenta las directrices trimestrales para el seguimiento al plan de acción institucional que emite la Oficina Asesora de Planeación, donde se detalla cómo se realiza*"

  Sin embargo en la Guía de Evaluación del Desempeño Institucional, Código: G-GES-ED-001, versión 1, en relación con la gestión de los riesgos en la entidad, se establece que: "*…además deberá informar si se han presentado eventos que haya materializado alguno de los riesgos que estén bajo su responsabilidad, con el fin de analizar las causas y establecer plan de acción en Isolución de ser necesario. Para los riesgos de corrupción la guía citada establece las acciones a realizar en caso de materialización*"; sin embargo, no se evidencia el establecimiento de un plan de acción en Isolución, entre otras para riesgos relacionados con la gestión de PQRSD en la cual se ha evidenciado la materialización del riesgo de oportunidad en la respuesta a las PQRSD.

- El seguimiento que se realiza no permite conocer la efectividad del control para evitar la materialización del riesgo.

Adicionalmente, en la Política de Administración de Riesgos, se indica que: "*Adicionalmente para los riesgos de corrupción, el jefe de Oficina de Control Interno, deberá adelantar seguimiento y en este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción*" y se pudo evidencia que a la fecha; al respecto, se evidenció su cumplimiento periódicamente y en el seguimiento realizado al plan de acción de la Oficina de Control Interno al 30 de septiembre, para la actividad relacionada con: "*Realizar (3) seguimientos al mapa de riesgos de corrupción y al PAAC. Con corte a 31 de diciembre de 2020, 30 de abril y 31 de agosto de 2021*"; en lo que tiene que ver con los riesgos, se informa lo siguiente:

> "*A Septiembre 30 esta meta se encuentra cumplida.*
> *Resultado del seguimiento:*
> *Análisis del Resultado:*
> *Objetivo: "Verificar el cumplimiento del Plan Anticorrupción y de Atención al Ciudadano – PAAC y evaluar la gestión de los riesgos de corrupción de la CGM con corte a 30 de agosto del 2021".*
> *Alcance: Seguimiento al PAAC y Riesgos de corrupción de la CGM con corte a 30 de agosto del 2021"*
> *Resultado:*
> *- La entidad tiene definidos seis (6) riesgos de corrupción los cuales se actualizaron para la vigencia 2021 bajo los lineamientos de la Guía para la Administración del Riesgo y Diseño de Controles versión 4 de la Función Pública. Además se evidenció que se encuentran en permanente revisión por parte de los líderes de los procesos lo que garantiza una oportuna actualización del mapa de riesgos de corrupción de la entidad.*
> *- Se realizó modificación a la matriz de riesgos en las siguientes dependencias: Subcontraloría riesgo CF-16, en las acciones para abordar riesgos números 340-341-342 y 343, toda vez que se ajustaron a la nueva guía y los roles de cada participantes en el proceso auditor.*
> *Secretaria General riesgo GRI-24: Se creó un nuevo control bajo la acción para abordar riesgos N° 383 y se cerraron las acciones N° 350 y 351.*
> *- Se continua con el seguimiento de los riesgos de Gestión y de Seguridad de la Información en el Módulo de Mejora del aplicativo Isolucion como "acciones para abordar riesgos"; lo anterior se debe a que* ***el sistema Isolución Módulo Riesgos, que es donde efectivamente se realiza el***

> ***seguimiento, no está actualizado de conformidad con la Guía para la Administración del Riesgo y Diseño de Controles de la Función Pública versión 5****, la cual depende de la gestión contractual con el proveedor del aplicativo*" (resaltado fuera de texto).

Al respecto es importante considerar la importancia de realizar el ajuste al aplicativo Isolución / Módulo de Riesgos, toda vez que actualmente se están utilizando archivos en Excel para los riesgos de gestión y de seguridad de la información; sólo se utiliza para los riesgos de corrupción.

Por último, consideramos importante que en la entidad se considere lo relacionado con la gestión de eventos y los indicadores clave de riesgo, conforme a lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, que se encuentran incluidos en el numeral 3.4 Herramientas para la gestión del riesgo.

# 8. CONCLUSIONES

## 8.1 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Frente a la determinación de la Política de Administración de riesgos, se identificó que debido al modelo de operación por procesos aprobado actualmente en la Entidad, en la que se llevó a cabo una simplificación de los procesos, y el establecimiento de puntos de control dentro de los procedimientos asociados a los 6 macro procesos, los cuales no son incluidos dentro de la matriz de riesgos de la Entidad, se podría no estar identificando y valorando la totalidad de los riesgos existentes en los procesos / procedimientos / proyectos que se ejecutan en la entidad conforme a la metodología establecida por la Función Pública.

Es importante articular las responsabilidades y directrices definidas para la Gestión de Riesgos, tanto para para la línea estratégica, así como para la primera, segunda y tercera línea, en la Política de Administración de Riesgos, con lo planteado en la Resolución 604 del 2020, la Política del Sistema de Control Interno y las funciones asignadas al Consejo de Dirección; igualmente, establecer y socializar una metodología relacionada con la Gestión del riesgo en la que se incluya, entre otros, el manual de manejo del sistema definido para la gestión del riesgo.

Se recomienda realizar periódicamente revisión a los niveles de tolerancia, aceptación o apetito del riesgo aceptados en la Entidad, entre otras, en lo relacionado a aquellos riesgos en los que el apetito del riesgo pueda ser cero, debido al impacto por perdida reputacional o económica debido al incumplimiento normativo.

Respecto a las actividades de seguimiento, revisión y monitoreo de los riesgos definidos en la matriz, no se tiene establecido en qué momento se debe realizar la revisión de los riesgos y la periodicidad de dicha revisión frente a la definición y diseño de los riesgos, en el que se incluya el análisis de aquellos aspectos relevantes sobre los factores de riesgo estratégicos para la Entidad; siendo importante fortalecer las actividades de revisión y monitoreo por parte de la segunda línea de defensa, llevando a cabo un seguimiento constante sobre la Gestión de Riesgo y la efectividad de los controles, en las que se establezca y se aplique periódicamente un monitoreo de las situaciones que representan un riesgo para la Entidad o se constituyan como riesgos ya materializados, a través de indicadores de riesgo (KRI), entre otros.

## 8.2 INSTITUCIONALIDAD PARA LA ADMINISTRACIÓN DEL RIESGO

**Línea Estratégica:** En la revisión realizada a las actas del Comité del Consejo de Dirección y al Comité Institucional de Coordinación de Control Interno, no se evidenció el cumplimiento de las actividades de "*seguimiento y **análisis periódico a la efectividad de los controles**", "Monitoreo permanentemente los riesgos de corrupción*" y "***Monitoreo al estado de los riesgos aceptados (apetito por el riesgo**), con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad".*

**Primera Línea de Defensa:** En el Manual de Políticas de Operación se incluyen responsabilidades a cargo de la primera línea de defensa, que no son claras como se ejecutan, toda vez que, entre otras, hacen alusión a verificaciones que se deben realizar a las actividades que tienen bajo su responsabilidad, por lo que serían juez y parte en estas, tales como verificación, en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas, verificación de la adecuada identificación de los riesgos relacionados con fraude y corrupción, y verificación de que el diseño del control establecido por la primera línea de defensa sea pertinente.

**Segunda Línea de Defensa:** Frente al monitoreo periódico del contexto estratégico por parte de la segunda línea de defensa, específicamente, por parte de la Oficina Asesora de Planeación, no se evidencia revisión del contexto estratégico previo a la aplicación de la Guía para la Gestión de Riesgos en 2021 y que fuera actualizada a Diciembre de 2020 por parte de la Función Pública, y la revisión de la exposición al riesgo con los grupos de valor diferente a los empleados. En relación con las actividades de revisión y monitoreo de los riesgos y los controles definidos, si bien se presentan los resultados consolidados de avance de cada una de las metas del Plan de Acción Institucional 2021, producto de las autoevaluaciones realizadas por la primera línea de defensa, no se evidencia algún pronunciamiento en relación con el diseño de los controles y que estos funcionen como se pretende, conforme a la política definida; adicionalmente, no se evidencia que se haya presentado en el CICCI lo relacionado con el riesgo de gestión de las PQRSD de acuerdo a lo planteado en el acta 3 de 2021 de Consejo de Dirección, en la que se informó la materialización del riesgo asociado al trámite de PQRSD, por incumplimiento de términos. Por lo anterior, es importante fortalecer la presentación de informes en el Comité Institucional de Coordinación de Control Interno, en relación con el monitoreo del contexto estratégico, la evaluación del diseño de los controles, su efectividad y que funcionen como se requiere, generando las alertas tempranas

requeridas por la entidad; así mismo, evaluar e informar sobre el cumplimiento de la Política de Administración del Riesgo.

Respecto al cumplimiento de las funciones asignadas a los Comités conformados en la Entidad y a la custodia de la información, se reitera lo mencionado en el Informe de Evaluación y Seguimiento al Cumplimiento de las Funciones Comités CGM; en la cual se plantea lo siguiente: *"Verificado el cumplimiento de las funciones de los comités establecidas en las diferentes resoluciones objeto de esta auditoría, se concluye que se debe tener especial cuidado en el cumplimiento de éstas y llevar registro de su desarrollo en las actas de las reuniones.* ***Se evidenció que algunos comités no estaban dando cumplimiento a sus funciones y/o no estaban dejando evidencia de la ejecución de las mismas****. Las acciones de los comités apoyan a la entidad en el cumplimiento de su misión, además de* ***generar las alertas oportunas en las dependencias para dar cumplimiento a los objetivos y metas estratégicas definidas por la entidad, y así garantizar la efectividad del Sistema de Control Interno de la Contraloría General de Medellín****".*

**Tercera Línea de Defensa:** El Manual de Políticas de Operación, establece para la Tercera Línea de Defensa, que debe: "*Asesorar de forma articulada con la Oficina Asesora de Planeación, sobre la identificación y diseño de controles a la primera línea (1 ª) y (2ª) línea de defensa"* y para la Segunda Línea de Defensa, que debe realizar un *"Trabajo coordinado con las Oficina de Control Interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno";* sin embargo no se tiene evidencia del cumplimiento de estas responsabilidades compartidas por parte de la Segunda y Tercera Línea; siendo importante tener en cuenta, que entre las recomendaciones que se han hecho de manera explícita durante los informes de evaluación a la gestión de riesgos y que han sido presentados en Consejo de Dirección, está el hecho de que se trabaje de manera articulada entre las Oficinas de Control Interno y la Oficina Asesora de Planeación, con el fin de que se consolide la gestión de riesgos al interior de la entidad.

## 8.3 APLICACIÓN DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS EN LA ENTIDAD

Para los riesgos de gestión, en lo relacionado con el análisis de objetivos estratégicos y de los procesos, no se observó inclusión de la meta específica relacionada con la Evaluación de las Políticas Públicas, en la Política Integral de Gestión y en la caracterización del Proceso Control Fiscal,
Tal como se plantea en el análisis DOFA realizado para el proceso control fiscal, se tiene identificado como amenaza para el ejercicio eficiente y eficaz del control fiscal

frente a los sujetos de control, la “Insuficiencia de personal idóneo con los perfiles adecuados y requeridos”; situación que podría impactar en el logro del objetivo estratégico.

Frente a la identificación de los puntos de riesgo en cada uno de los procesos institucionales, esta oficina reitera lo planteado en Consejo de Dirección, Acta 05 del 27/05/2021, frente a la definición y documentación de los procesos: *“la OCI ha evidenciado que falta una mayor claridad en la secuencia de las actividades que interactúan, la responsabilidad que se asigna a cada una de ellas y los requerimientos que hay entre sí, para su suficiente funcionamiento; considera que el alcance de los procesos dada la magnitud que hoy tienen, cobijan actividades que pueden distar de su objeto, de su naturaleza, de su responsabilidad, inclusive de su riesgo, notando dificultad en su administración”.*

Respecto a los hallazgos generados durante las evaluaciones realizadas por la Auditoría General de la República AGR, auditorías internas de calidad, y la Oficina de Control Interno, los cuales podrían señalar puntos de riesgo para la Entidad, no se evidencia revisión y ajuste de los controles establecidos para los riesgos definidos, o en su defecto, identificación de nuevos riesgos; así mismo, no se evidencian riesgos y controles relacionados con la continuidad del negocio.

En lo relacionado con la identificación de las áreas de impacto, sería importante profundizar en la definición de las consecuencias que se generan debido a la materialización de los riesgos, tales como la pérdida de la certificación por parte de la Auditoría General de Republica, y la posible intervención administrativa por parte de la Contraloría General de la República, debido a que el índice AuditeCT para la contraloría, sea menor al puntaje crítico de certificación anual, conforme a la metodología definida por la Auditoría General de la República, lo cual podrían implicar cambios en los niveles de impacto asociados a cada uno de los riesgos. Frente a la identificación de áreas de factores de riesgo, se plantea lo siguiente en la Política de Administración de Riesgos de la Entidad “…los factores de riesgos como procesos, talento humano, tecnología, infraestructura y eventos externos…”; sin que se dé información adicional sobre su definición y una descripción de dichos factores o que se hayan considerado otros adicionales, conforme a lo planteado en la guía.

Una vez analizados los riesgos asociados a los procesos institucionales, se evidenció lo siguiente frente a la identificación de riesgos:

- ✓ No se realizó una revisión previa del contexto estratégico y matriz DOFA para la definición de los riesgos y causas.
- ✓ No se profundiza en las posibles causas y subcausas que permitan posteriormente identificar con mayor claridad los controles requeridos.
- ✓ Las causas inmediatas no corresponden conforme a la estructura propuesta para la redacción de riesgos
- ✓ Se mezcla la causa inmediata con la causa raíz
- ✓ La causa raíz describe una situación general, sin que se identifiquen subcausas relacionadas.

Lo anterior, permite concluir que existen debilidades en la estructuración del riesgo, conforme a la metodología definida por la Función Pública; así mismo es necesario, profundizar en las subcausas, con el fin de poder posteriormente establecer los controles pertinentes.

Es importante tener en cuenta en la identificación del riesgo, lo planteado en la guía, "*No existen riesgos transversales, lo que pueden existir son causas transversales.* ***Ejemplo:*** *pérdida de expedientes. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes*"

Por lo cual, es importante revisar aquellos riesgos que se pueden presentar en diferentes procesos; entre otros lo relacionado con la Rendición de la Cuenta y la gestión de las PQRSD; inclusive el ejemplo propuesto relacionado con Gestión Documental.

Adicionalmente, en la revisión realizada no se evidenciaron riesgos de fraude, que conforme a lo establecido en la metodología, entre otros, el fraude interno corresponde a "Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros" y que entre otros, podría estar relacionado con información financiera fraudulenta o apropiación indebida de activos.

En relación a los riesgos de seguridad de la información definidos en la Entidad, se puede concluir que si bien se tienen identificados riesgos relacionados con pérdida de la confidencialidad, pérdida de integridad y pérdida de disponibilidad, se debe dar aplicación a la Guía para la Administración del Riesgo y el Diseño de Controles

en Entidades Públicas, versión 5; en la cual se establece que “para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso”; para a partir de allí establecer los demás elementos pertinentes a la metodología, entre otras la definición del nivel de criticidad partiendo de la criticidad respecto a la confidencialidad, la integridad y la disponibilidad del activo de los procesos.

En relación con la probabilidad y el impacto definidos, se identificó lo siguiente durante las reuniones realizadas con las dependencias:

- ✓ En caso de considerarse en el impacto la posible pérdida de la certificación anual por parte de la AGR por incumplimiento de metas y objetivos, o los efectos sobre la imagen institucional frente a otras partes interesadas a nivel regional y nacional, el impacto inherente en algunos riesgos afectaría la imagen de la Entidad a nivel nacional, con lo que el impacto del riesgo se ubicaría en una zona de riesgo inherente en una escala mayor a la que actualmente se encuentra.
- ✓ En algunos casos, la frecuencia identificada para la actividad en la que se evidencia exposición al riesgo o el número de veces en las que se pasa por el punto de riesgo, no corresponde a lo establecido en la Guía de Administración de Riesgos.
- ✓ En algunos casos, no es clara la fuente o base para determinar el impacto (posible afectación económica, entes sancionadores, entre otros).

Frente a la evaluación del riesgo, en la definición de los controles asociados, se pudo evidenciar, entre otras, lo siguiente:

- ✓ Existen controles que se encuentran definidos en las diferentes políticas de operación, que no fueron tenidos en cuenta al momento de analizar los controles relacionados con el riesgo.

- ✓ Se debe garantizar el cumplimiento de la metodología al momento de definir los diseñar los controles

- ✓ Dado que los controles correctivos, permiten disminuir el impacto de los riesgos; es importante profundizar en los posibles controles para los riesgos pertinentes en la entidad.

- ✓ Es importante tener en cuenta el control establecido en la Guía de Liberación de Productos y Control de Salidas No Conformes, Código:G-GES-LPC-001,

Versión 4, en la que se establece que: "*La Liberación aplica para los productos definidos en la entidad en temas misionales y el control de salidas no conformes aplica para todas las salidas de los procesos…*", en especial, porqué en ella se establecen las acciones a seguir cuando se evidencia una salida no conforme.

- ✓ Entre las estrategias definidas para combatir el riesgo, se encuentra el trasferir, en el que "*después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas*" y en ninguno de los casos se evidenció la transferencia del riesgo.

Finalmente, una vez analizados los seguimientos realizados de manera trimestral en el módulo de Riesgos de Isolución, se pudo evidenciar lo siguiente:

- ✓ No existen directrices específicas de lo que debe contener el seguimiento que se realiza; lo anterior, toda vez que en un alto número de acciones para abordar los riesgos, el seguimiento que se realiza es el mismo cada trimestre; sólo se cambian algunos datos.

- ✓ Los seguimientos que se realizan, en algunos casos son iguales a la actividad que se plantea.

- ✓ En el seguimiento que se realiza a algunas acciones para abordar los riesgos, se indica que no se ha materializado el riesgo; sin embargo en la Política de Administración de Riesgos no se dan lineamientos frente a las gestiones que se deben adelantar en caso de materialización de los riesgos; solamente se plantea para los procesos contractuales, que "la Secretaria General consolidará estos resultados y la posible materialización de algún riesgo, de lo cual presentará informe ante el Consejo de Dirección".

- ✓ El seguimiento que se realiza no permite conocer la efectividad del control para evitar la materialización del riesgo.

Por último, es importante que en la entidad se considere lo relacionado con la gestión de eventos y los indicadores clave de riesgo, conforme a lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, que se encuentran incluidos en el numeral 3.4 Herramientas para la gestión del riesgo

## 9. RECOMENDACIÓN

Atendiendo las observaciones y conclusiones planteadas en el presente informe, se recomienda realizar capacitación y/o asesoría a nivel institucional en lo relacionado con la implementación de la Guía de Administración y Gestión de riesgos del DAFP, definición y aplicación de la Política de Administración de riesgos en articulación con el esquema de líneas de defensa, niveles de aceptación del riesgo, análisis del contexto estratégico de los procesos, identificación de los riesgos y sus causas, identificación de los niveles de impacto y probabilidad, diseño de los controles, seguimiento a las actividades de control, monitoreo a las actividades de tratamiento o planes de acción definidos en caso de identificarse materialización de los riesgos, definición de indicadores de riesgo, entre otros