ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SEGURIDAD,
CONVIVENCIA Y JUSTICIA

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE
SEGURIDAD, CONVIVENCIA
Y JUSTICIA
BOGOTÁ

1. OBJETIVO

Suministrar las pautas para la Administración del Riesgo de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ permitiendo identificar, analizar, controlar y mitigar los Riesgos de Gestión, Riesgos de Corrupción (incluyendo los Riesgos asociados a Lavado de Activos y Financiación del Terrorismo - LA/FT), Riesgos de Seguridad de la Información, Riesgos Estratégicos y Riesgos Fiscales; que podrían afectar de manera negativa el logro de los objetivos estratégicos de la Entidad, impidiendo la oferta adecuada, efectiva y optima de los servicios a la ciudadanía para los cuales fue concebida la SDSCJ. Propendiendo el desarrollo, implementación y mejora continua de la Entidad en procesos globales, estrategia y planificación, gestión, procesos de presentación de informes, políticas, valores y cultura organizacional protegiendo el valor de la organización.

En este sentido, la SDSCJ procede con la adopción de la presente Política y la Guía de Administración de Riesgos al interior de la Entidad basados en los lineamientos impartidos en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6" del Departamento Administrativo de la Función Pública – DAFP emitida en noviembre de 2022, como lineamiento en la implementación de la administración de los Riesgos de Gestión, Riesgos de Corrupción, Riesgos de Seguridad de la Información y Riesgos Fiscales.

A su vez, se apropia el "Documento Técnico - Adaptación de Medidas de Prevención y Mitigación del Riesgo del Lavado de Activos, Financiación del Terrorismo en las Entidades del Distrito Capital." emitido por la Secretaría General de la Alcaldía Mayor de Bogotá D.C. la cual indica que las Entidades privadas o públicas de índole nacional o territorial deben diseñar sistemas de administración de riesgos que les permita protegerse ante el riesgo asociado al lavado de activos (LA) y Financiación del Terrorismo (FT) y de esta forma dar cumplimiento a las obligaciones que se establecen en la normatividad vigente. Lo anterior, para evitar que sean utilizadas en el proceso de lavado de activos y financiación del terrorismo. Así entonces, la Entidad acoge la recomendación de asociar y articular a la gestión de riesgos de Corrupción, los criterios para la identificación, análisis y evaluación de riesgos asociados a LA/ FT.

A su vez, como complemento a la presente Política, la Entidad formula el Plan de Cultura e Integridad, en el cual se compromete con la integridad y trasparencia en las actuaciones de sus servidores, centrando su gestión en función de los ciudadanos para lograr la confianza de estos con el estado y con la Entidad, impactando el logro de los objetivos institucionales mediante una cultura de Integridad consistente. Por ello se fomenta la apropiación del Código de Integridad de la Entidad del Distrito, en cada uno de los servidores, resaltando el cumplimiento de la promesa de ejercer a cabalidad su labor, alineada al Modelo Integrado de Planeación y Gestión - MIPG, para guiar a sus servidores públicos en el ejercicio de una gestión institucional moderna, eficiente, transparente, generando seguridad al servicio de nuestros grupos de valor y reestablecer la confianza en la función pública. Mediante el plan se promueve, que nuestros servidores públicos reflejen en sus actuaciones y contribuciones la lucha contra la corrupción y la necesidad de aumentar los niveles de transparencia de la Entidad, generando credibilidad en la comunidad en general.

La presente Política se enfoca en el objetivo de identificar, analizar, dar tratamiento, seguimiento y evaluación a los riesgos, logrando una visión integral de las actividades propias de la Entidad que podrían afectar el cumplimiento de las metas y objetivos trazados.

La Gestión del Riesgo en la SDSCJ se complementa con la Gestión de las Oportunidades, donde se identifican y desarrollan acciones que la Entidad y los procesos deben aprovechar para mejorar su desempeño articulados a lo definido en el Contexto estratégico de la Entidad, así como los Riesgos Estratégicos asociados a los Objetivos Estratégicos de la Entidad.

2. ALCANCE

Esta política busca puntualizar los lineamentos y criterios para la identificación, el análisis, el control, el seguimiento de los Riesgos Estratégicos, Riesgos de Gestión, de Corrupción (contemplando SARLAFT), Riesgos de Seguridad de la Información, Riesgos Fiscales y la Gestión de Oportunidades en la SDSCJ, contando con el análisis de factores internos y externos. La administración del riesgo inicia desde la identificación del contexto del riesgo hasta el seguimiento, tratamiento y comunicación de la información resultante de la administración de este; desarrollado mediante la Guía de Administración del Riesgo de la Entidad que adopta los lineamientos impartidos en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6" del Departamento Administrativo de la Función Pública – DAFP.

Los riesgos de seguridad de la Información se gestionarán de acuerdo con los criterios diferenciales de la Política de Seguridad y Privacidad de la Información.

3. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, asume el compromiso de administrar los Riesgos de Gestión, Riesgos de Corrupción, Riesgos de Seguridad Información, Riesgos Estratégicos y Riesgos Fiscales; que puedan afectar de manera negativa el alcance de los objetivos estratégicos y de procesos de la Entidad; además de forjar una Entidad preventiva, proactiva y detectiva, que trabaje en la reducción de los efectos no deseados y promoviendo la mejora continua, proyectando así, una organización basada en la acción preventiva automática, que controla todos los procesos de la Entidad, brindando seguridad razonable y destinando los esfuerzos y recursos necesarios para administrar los riesgos que se puedan presentar en la SDSCJ.

Lo anterior, fundamentado en la determinación de la capacidad del riesgo, el nivel de apetito del riesgo y la tolerancia del riesgo en la Entidad.

La administración del riesgo se complementa con la gestión de las oportunidades, donde se identifican las situaciones positivas que los procesos deben aprovechar para mejorar el desempeño y acciones proyectadas.

4. NORMATIVIDAD

TIPO	DESCRIPCIÓN	EMITE/AUTOR
Artículo 73 de la Ley 1474 de 2011	Relacionado con la prevención de los riesgos de corrupción, - mapa de riesgos de corrupción.	Congreso de la República
Ley Estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Congreso de la República
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	Congreso de la República
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.	Presidencia de la Republica
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 y se establece el MIPG	Presidencia de la Republica
Decreto 648 de 2017	Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública	Presidencia de la Republica
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 del 2015, decreto único reglamentario del sector de tecnologías de la información y las telecomunicaciones.	Presidencia de la Republica
Resolución 500 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.	Ministerio de las Tecnologías de la información y las comunicaciones
CONPES 3854 del 11 de abril de 2016, 3.2. Estrategia de gestión de riesgos de seguridad digita	El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad de la información, teniendo en cuenta el marco.	Consejo nacional de política económica y social república de Colombia Departamento Nacional de Planeación

TIPO	DESCRIPCIÓN	EMITE/AUTOR
Decreto 610 de 2022	Por medio del cual se adopta el Modelo de Gestión Jurídica Anticorrupción para el Distrito Capital y se dictan otras disposiciones	Alcaldía Mayor de Bogotá, D.C.
LEY No. 2195 DE 2022	Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.	Congreso de la República

Tabla 1, Elaboración propia

5. DOCUMENTOS ASOCIADO

- PO-FI-1 Política de Administración de Riesgos
- F-DE-1379 Matriz de Contexto Estratégico
- F-FI-1382 Matriz general de Riesgos por Proceso
- F-FI-1384 Matriz general de Riesgos de Corrupción
- F-FI-1385 Matriz de Riesgos de Seguridad de la Información
- F-FI-1383 Matriz de Identificación Calificación y Seguimiento de Oportunidades
- G-FI-04 Guía de Administración del Riesgo

6. GLOSARIO

Ver Guía de Administración del Riesgo.

7. TIPOS DE RIESGOS QUE SE VAN A CONTROLAR

Los tipos de riesgo a controlar en la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ en la presente Política de Administración de Riesgos, son:

- Riesgos Estratégicos
- Riesgos de Gestión
- Riesgos de Corrupción junto a Riesgos asociados a LAFT
- Riesgos de Seguridad de la Información
- Riesgos Fiscales
- Oportunidades

En la Guía de Administración del Riesgo se detalla la metodología para administrar cada uno de estos riesgos.

8. ROLES, RESPONSABILIDADES, COORDINACIÓN Y ARTICULACIÓN

En cumplimiento de la normatividad proferida para la implementación del Modelo Integrado de Planeación y Gestión - MIPG en las Entidades de la Administración Distrital y las disposiciones del Decreto 1499 de 2017 (que modifica al Decreto 1083 de 2015 por el cual se actualiza el MECI incluyéndolo de manera integral con el anterior Sistema Integrado de Gestión en el nuevo Modelo Integrado de Planeación y Gestión) 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 para una adecuada gestión del riesgo) las Entidades públicas deben estructurar lineamientos que orienten la toma de decisiones para el manejo y tratamiento de los riesgos identificados en los procesos, para lo cual la Secretaría Distrital de Seguridad, Convivencia y Justicia ha determinado los siguientes aspectos:

8.1 Roles y Responsabilidades

La Política de Administración del Riesgo es responsabilidad de todas las personas naturales y jurídicas contemplando servidores y colaboradores que componen la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, así como, la implementación de una gestión adecuada de los Riesgos de Gestión, Riesgos de Corrupción, Riesgos de Seguridad de la Información, Riesgos Estratégicos, Riesgos asociados a LAFT y Oportunidades; la SDSCJ debe efectuar la formulación de la matriz respectiva con una participación integral y activa del líder del proceso y el líder operativo los cuales deben contar con el apoyo de los funcionarios y contratistas que hacen parte del proceso.

8.2 Las líneas de defensa:

De acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión - MIPG en la Dimensión 7 de Control Interno, y lo definido en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Riesgos de Gestión, Corrupción y Seguridad de la Información” del Departamento Administrativo de la Función Pública, para la correcta operación se requiere del esquema de líneas de defensa el cual es soportado por la creación 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, permitiendo una adecuada gestión del riesgo, dicha institucionalidad funciona de la siguiente forma:

LÍNEA ESTRATÉGICA

Define el marco general para la gestión del riesgo contemplando su control y supervisión de su cumplimiento, está a cargo de la Alta Dirección, incluyendo el Comité de Coordinación de Control Interno y apoyados por el Comité Institucional de Gestión y Desempeño.

La responsabilidad se centra en la definición, emisión, revisión, validación, supervisión y evaluación del cumplimiento de la presente Política, considerando su aplicación, cambios en el entorno y las dificultades para su desarrollo mediante los reportes periódicos que son emitidos por la Segunda y tercera línea de defensa

Se propende asegurar el ambiente de control permitiendo a la Entidad disponer de las condiciones mínimas para el ejercicio de control interno.

- **COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO:** En este comité se analiza la gestión del riesgo y se aplican las mejoras.
- **COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO:** Corresponde al Comité de Control Interno aprobar y en caso de ser pertinente, modificar la Política de administración del Riesgo, en cumplimiento a la resolución 215 de 2017. Debe asegurar su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo. En este comité debe efectuar el análisis de eventos y riesgos críticos.

PRIMERA LÍNEA DE DEFENSA

Comprende al Secretario, Subsecretarios, Jefes de Oficina, funcionarios y contratistas que efectúan las actividades que permiten el cumplimiento de los objetivos estratégicos de la Secretaría y de los procesos. Corresponde a los Líderes de Proceso y Líderes Operativos asegurarse de implementar la presente Política para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. A su vez, para todo tipo de riesgos debe garantizar el monitoreo y revisión periódica; en caso de ser necesario algún ajuste debe coordinar dicha gestión con la Segunda Línea defensa. Será su responsabilidad dar reporte de la materialización de los riesgos a la Segunda y Tercera línea de Defensa, así como, el cumplimiento del reporte y cargue de evidencias en los repositorios de información destinados para ello en los tiempos estipulados por la Oficina Asesora de Planeación y lo mencionado en el presente documento.

El Gestor de Riesgos será desempeñado por el Líder Operativo de cada proceso.

SEGUNDA LÍNEA DE DEFENSA

Corresponde a la Oficina Asesora de Planeación ejecutar la consolidación de la gestión del riesgo estratégico, de gestión, corrupción y Fiscales, así como la difusión y asesoría de la presente metodología, junto al tratamiento de los riesgos identificados en todos los niveles de la Entidad, de tal forma que se asegure su implementación. Capacita, acompaña, genera recomendaciones a la primera línea con base en los lineamientos definidos.

La Dirección de Tecnologías y Sistemas de la Información consolida la información de la gestión del riesgo de seguridad de la información, así como la difusión y asesoría de la presente metodología, junto al tratamiento de los riesgos identificados en todos los niveles de la Entidad, de tal forma que se asegure su implementación. Capacita, acompaña, genera recomendaciones con base a los lineamientos definidos.

El jefe de Gestión humana, como instancia de segunda línea de defensa es el encargado de monitorear temas clave del ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral, código integridad), generando alertas sobre incumplimientos,

situaciones críticas que afectan en clima laboral y posibles afectaciones al código de integridad

TERCERA LÍNEA DE DEFENSA

Le corresponde a la Oficina de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la Entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la Entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

- Asesorar en coordinación con la Oficina Asesora de Planeación y la Oficina de Tecnología, a la primera línea de defensa en la análisis y valoración del riesgo, y en el diseño de los controles.
- Verificar la publicación de los mapas de riesgos en la página web de la Entidad.
- Realizar seguimiento a la gestión de riesgos (análisis de causas, riesgos, eficacia y efectividad de los controles), en los procesos que realice de auditorías internas.
- Recomendar mejoras a la política de administración del riesgo.
- Realizar evaluación a la gestión de Riesgos de la Entidad.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Adicional a las líneas de defensa anteriormente mencionadas y en concordancia con lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones y en la Política de Seguridad y Privacidad de la Información, la SDSCJ delega la responsabilidad de gestionar los riesgos de seguridad de la información al encargado de los siguientes compromisos:

- Gestionar los Riesgos de Seguridad de la Información (identificación, análisis, formalización, evaluación y tratamiento)
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento al tratamiento de los riesgos definidos.
- Presentar a la mesa técnica de Seguridad Digital para que esta a su vez presente a la línea estratégica.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

9. DERECHOS DE AUTOR

Todas las referencias a los documentos de la Política de Administración de Riesgos son derechos reservados por parte de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ.

En consecuencia, la SDSCJ goza de los derechos de autor establecidos en Ley 1915 de 2018 que modifica y adicional la Ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos de la Política de Administración de Riesgos.

10. METODOLOGIA A IMPLEMENTAR

La Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ efectúa la aplicación de la Metodología para la Administración de Riesgos ejecutando los tres (3) pasos básicos establecidos por la Guía del DAFP en caso de evidenciar alguno de los siguientes cambios: (1) en el contexto de la Entidad o de los procesos, (2) relacionados con el “Conocimiento de la Entidad” o (3) del “Modelo de Operación por Procesos”. El ejercicio culmina con la oficialización y publicación de las Matrices por parte de la Oficina Asesora de Planeación con las cuales se inicia la gestión del año complementado por estrategias de comunicación a toda la Entidad.

El ejercicio se complementa con la realización de un análisis del estado de la estructura de riesgos y su gestión en la Entidad al cierre de cada año, esta actividad se desarrolla durante el primer trimestre posterior al cierre del año.

A continuación, se puede observar la estructura completa para cumplir satisfactoriamente con el objetivo de la correcta administración del riesgo, se hace necesario seguir los siguientes pasos:

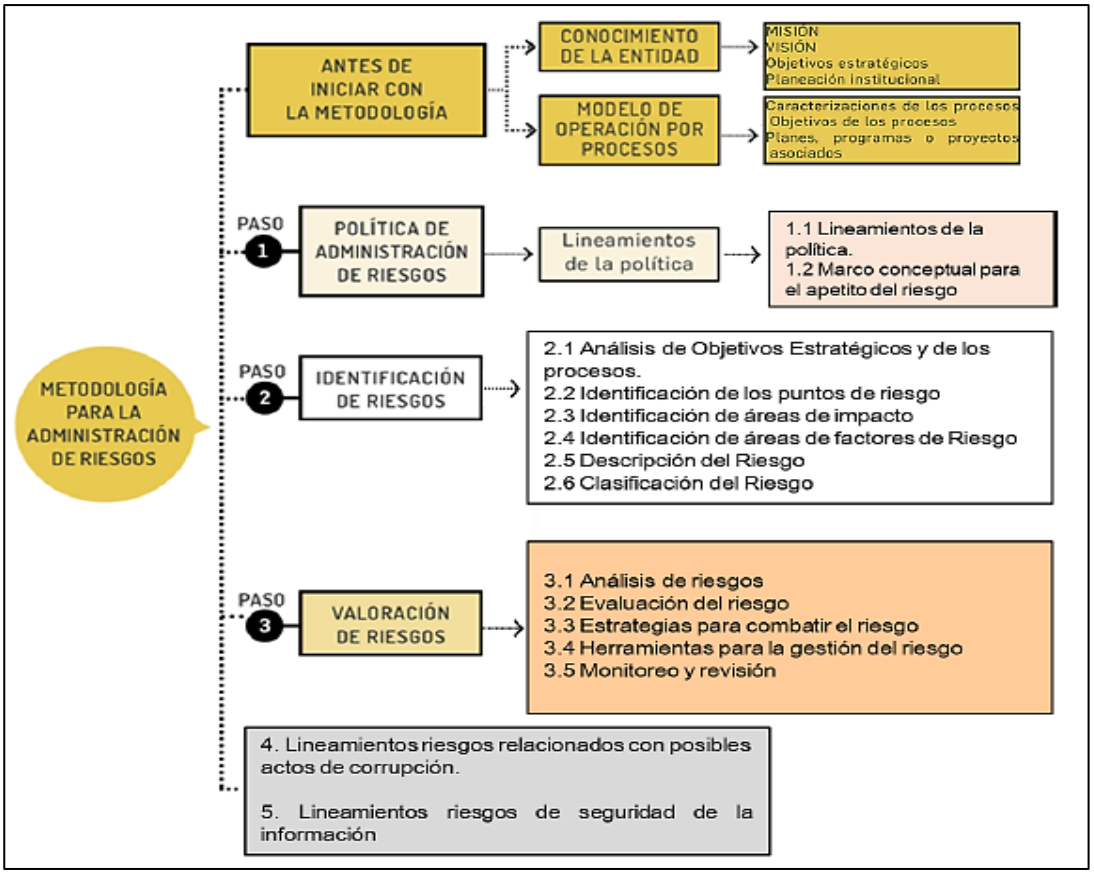

Ilustración 1, Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas. Versión 6

11. IDENTIFICACIÓN Y GESTIÓN DEL RIESGO

Partiendo de lo expuesto en el numeral anterior, el análisis de riesgos y la aplicación de la metodología en general, se desarrolla por pasos permitiendo la gestión adecuada del Riesgo, destacando la obligatoria participación del líder de proceso o líder operativo, quienes a su vez están a cargo de realizar una apropiada socialización con los funcionarios y contratistas que componen cada proceso.

11.1 Conocimiento y divulgación de la Política de Administración de Riesgos

La presente Política debe ser de conocimiento general para los funcionarios y contratistas de la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, se debe tener en cuenta que en este documento se plantean los lineamientos y en la Guía de Administración del Riesgo se especifican los lineamientos técnicos con los cuales se ejecutan las actividades en la Entidad, por ende toda persona que interactúe con procesos y procedimientos debe participar activamente en función a la Gestión del Riesgo, considerando su conocimiento, percepciones y experiencia, propendiendo la mejor decisión evitando las posibles afectaciones y consecuencias por el desarrollo de actividades.

11.2 Apetito, Tolerancia y Capacidad del Riesgo de Gestión

El Apetito del Riesgo, Tolerancia del Riesgo y Capacidad del riesgo se detalla al interior de cada uno de los numerales de cada uno de los tipos de Riesgo en la “Guía de Administración del Riesgo”.

11.3 Tratamiento de Riesgo

Dada la Zona de Riesgo Residual obtenida con la ejecución de controles, se realiza un tratamiento a los riesgos identificados que se aplica de la siguiente forma:

- **Aceptar el riesgo:** Valido únicamente para aquellos cuya Zona de Riesgo Residual es Baja no se aplica ninguna acción adicional a la ejecución permanente del control que se tiene estipulado asumiendo el mismo conociendo los efectos de su posible Materialización. **No Aplica para Riesgos de Corrupción.**
- **Reducir el riesgo:** Para aquellos cuya Zona de Riesgo Residual sea diferente a Baja, se deberán toman acciones mediante Transferencia o Mitigación previa realización de un análisis de la situación dejando evidencia en la Matriz de Riesgos:
  - **Mitigar:** Esto se logra por medio de acciones que mitiguen el nivel de Riesgo, no necesariamente se refiere a la implementación de controles adicionales.
  - **Transferir:** Estrategia de tercerización del proceso o traslado del riesgo a través de Seguros o Pólizas. La Responsabilidad económica recaerá sobre el tercero. Sin embargo, se mantiene la Responsabilidad reputacional.
- **Evitar el riesgo:** Se determina no asumir el riesgo por lo cual se elimina la ejecución de las actividades que faciliten la materialización.

Todos los riesgos deben contar con algún tratamiento residual independiente de la Zona de Riesgo. Al interior de la "Guía de Administración del Riesgo" se detalla el tratamiento para cada tipo de Riesgo

12. ACCIONES POR SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

En caso de presentarse la materialización de un riesgo, el líder de proceso con el apoyo del Líder Operativo realiza el análisis de causas y ajustes necesarios al mapa de riesgos con el acompañamiento metodológico de la Oficina Asesora de Planeación, junto con las siguientes medidas de acuerdo con el tipo de riesgo materializado:

TIPO DE RIESGO	ACCIONES
Riesgos de Gestión, Riesgos de Seguridad de la Información y Riesgos Estratégicos	La primera línea debe informar a la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias mediante correo electrónico o memorando. Efectuando una descripción detallada de lo ocurrido contemplando el impacto generado a los objetivos del proceso y la Entidad por la materialización del riesgo.
	La primera y Segunda línea deben revisar la identificación y valoración del riesgo, analizando las causas que lo generaron y los controles existentes, con el fin de disminuir la posibilidad de una nueva materialización del riesgo documentando el ejercicio mediante acta de reunión.
	La primera línea con el apoyo de la Segunda línea debe basado en el diagnóstico de la situación presentada, formular y establecer un plan de acción documentado en el mapa de riesgos. Así como identificar y ejecutar las acciones correctivas.
	La segunda línea de defensa (OAP) debe llevar a cabo un monitoreo mensual de las actividades propuestas hasta que las mismas finalicen, a su vez incluirá el evento presentado en el Histórico de Eventos Materializados que se refleja en el Informe periódico.
	La Tercer línea de defensa (OCI) evalúa que los controles sean efectivos y oportunos, y atiendan el riesgo formulado.
Riesgos de Corrupción, Fiscales	La primera línea debe informar a la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias mediante correo electrónico o memorando. Efectuando una descripción detallada de lo ocurrido contemplando el impacto generado a los objetivos del proceso y la Entidad por la materialización del riesgo.
	La primera línea con el apoyo de la Segunda línea debe basado en el diagnóstico de la situación presentada, establecer un plan de acción documentado en el mapa de riesgos. Así como identificar y ejecutar las acciones correctivas.
	La segunda línea de defensa (OAP) debe llevar a cabo un monitoreo mensual de las actividades propuestas hasta que las mismas finalicen, a su vez incluirá el evento presentado en el Histórico de Eventos Materializados que se refleja en el Informe periódico.
	La segunda y la tercera línea de defensa deben verificar si se diseñó y ejecutó el plan de acción y se actualizó el mapa de riesgos.
	La línea de defensa que identifique la materialización del riesgo debe informar a las autoridades internas y externas de la ocurrencia del hecho. Para realizar dicho reporte, se debe contar con la asesoría y apoyo de la Dirección Jurídica y Contractual para el desarrollo de la notificación.
	La Tercer línea de defensa (OCI) debe evaluar que los controles sean efectivos y oportunos, y atiendan el riesgo formulado.

Tabla 2, Elaboración propia

El resultado del ejercicio debe socializarse a la Línea Estratégica mediante el Comité Institucional de Coordinación de Control Interno, escenario en el que se debe establecer si es necesario algún tipo de reporte ante los organismos de control. La presentación ante el comité de la materialización del Riesgo será responsabilidad de la línea de defensa que detecte la materialización.

Para los eventos asociados al ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral, código integridad) respecto a la integridad y trasparencia conforme a las actuaciones de sus servidores impactando el logro de los objetivos institucionales se actúa de acuerdo con lo establecido en el Código de Integridad de la entidad ejercicio que efectúa la Dirección de Gestión Humana.

Los siguientes también son considerados como canales de información para la detección de materializaciones de Riesgos:

- Mesa de ayuda de tecnología a nivel interno
- Información del área o proceso de atención al usuario
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia
- Mecanismo interno establecido para que cada líder de proceso haga el reporte cuando se presenta un evento

13. PUBLICACIÓN, SEGUIMIENTO Y EVALUACIÓN A LOS RIESGOS

Con el fin de dar cumplimiento a lo indicado en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6” del Departamento Administrativo de la Función Pública – DAFP y con el objetivo de implementar un monitoreo efectivo para la adecuada administración de los riesgos en la SDSCJ, corresponde a los líderes de procesos y líderes operativos realizar la revisión y seguimiento de sus respectivos mapas de riesgos, ejercicio de autocontrol que debe ser continúo, permanente y consistente con la ejecución de las actividades proyectadas en las matrices de Riesgos.

La versión vigente de las Matrices será la última publicada tanto en la Página WEB de la SDSCJ, lo cual debe estar respaldado por lo compilado en el sistema Portal MIPG que administra la Oficina Asesora de Planeación.

Las Matrices deben ser publicadas y divulgadas en la página web de la Entidad junto con los informes de seguimiento en el espacio de “Transparencia y Acceso a la Información Pública” / “Planeación, Presupuesto e Informes” / “Plan de acción”.

Todo riesgo debe ser aprobado por el líder de proceso, y el reporte debe ser realizado por el Líder operativo. El ejercicio de cargue, monitoreo y evaluación se efectúa en el repositorio de información designado por la Oficina Asesora de Planeación.

La Dirección de Gestión Humana Respecto realiza el seguimiento a las alertas generadas conforme al monitoreo institucional por las posibles afectaciones a la integridad y trasparencia como consecuencia de las actuaciones desarrolladas por sus servidores, mediante lo establecido en el Código de Integridad de la Entidad.

A continuación, se detallan las responsabilidades, actividades y fechas para la gestión de los Riesgos:

Responsable	Tipo de Riesgo				
	Gestión	**Corrupción/Fiscales**	**Seguridad de la Información**	**Oportunidades**	**Estratégicos**
Primera Línea de Defensa	Realizan la ejecución de los controles y los eventos de riesgo del proceso.				
	Los Líderes Operativos realizan el cargue de soportes documentales de la implementación de los controles a más tardar el 5° día hábil luego de vencido el Trimestre.	Los Líderes Operativos realizan el cargue de soportes documentales de la implementación de los controles a más tardar el 3° día hábil luego de vencido el cuatrimestre.	Los Líderes Operativos realizan el cargue de soportes documentales de la implementación de los controles a más tardar el 5° día hábil luego de vencido el cuatrimestre.	Los Líderes Operativos realizan el cargue de soportes documentales de la implementación de los controles a más tardar el 10° día hábil luego de vencido el semestre.	Los Lideres Operativos realizan el cargue de soportes documentales de la implementación de los controles a más tardar el 10° día hábil luego de vencido el semestre.
Segunda Línea de Defensa	Realiza revisión de los soportes documentales de la implementación de los controles en el repositorio de información correspondiente.				
	Corresponde a la Oficina Asesora de Planeación. Realiza trimestralmente seguimiento a la Matriz de Riesgos y remitirá informe del resultado a la Oficina de Control Interno, los primeros 10 días hábiles, una vez vencido el trimestre.	Corresponde a la Oficina Asesora de Planeación. Realiza cuatrimestralmente seguimiento a la Matriz de Riesgos y remitirá informe del resultado a la Oficina de Control Interno, los primeros 5 días hábiles, una vez vencido el cuatrimestre.	Corresponde al Oficial de Seguridad de la Información de la Dirección de Tecnologías y Sistemas de la Información. Realiza cuatrimestralmente seguimiento a la Matriz de Riesgos y remitirá informe del resultado a la Oficina de Control Interno, los primeros 10 días hábiles, una vez vencido el cuatrimestre.	Corresponde a la Oficina Asesora de Planeación. Realiza semestralmente seguimiento a la Matriz de Riesgos y remitirá informe del resultado a la Oficina de Control Interno, los primeros 15 días hábiles, una vez vencido el semestre.	Corresponde a la Oficina Asesora de Planeación. Realiza semestralmente seguimiento a la Matriz de Riesgos y remitirá informe del resultado a la Oficina de Control Interno, los primeros 15 días hábiles, una vez vencido el semestre.
Tercera Línea de Defensa	Evalúa las matrices de riesgo y el informe de seguimiento, verificando que la información cumpla con los lineamientos expresados en la política y Guía de Administración de Riesgos. De encontrar desviaciones genera recomendaciones u observaciones con el objetivo de mejorar su efectividad.				
	Realiza informe en los siguientes cortes: Cuarta semana de mayo, Cuarta semana de agosto, Cuarta semana de noviembre y Cuarta semana de febrero.	Realiza informe en los siguientes cortes: A los 10 días hábiles de mayo, a los 10 días hábiles de septiembre y a los 10 días hábiles de enero	Realiza informe en los siguientes cortes: Tercera semana de junio, Tercera semana de octubre y Tercera semana de febrero	Realiza informe en el siguiente corte: Según el Plan Anual de Auditoría	Realiza informe en los siguientes cortes: Cuarta semana de agosto y Cuarta semana de febrero

Tabla 3, Elaboración propia

Los resultados de los Informes de Seguimiento y evaluación de los Riesgos serán socializados y divulgados en el Comité de Gestión y Desempeño.

Los informes elaborados por la Oficina Asesora de Planeación deben contener como mínimo el siguiente contenido: la confirmación de la versión de la Matriz objeto de seguimiento, la relación de los cambios efectuados en las matrices de Riesgos, confirmación de la cuantificación de Riesgos y controles, análisis de la gestión del Riesgo en el periodo comparando las zonas de Riesgos Inherentes vs Residual, seguimiento a los materializados y las acciones vigentes, confirmación de la oportunidad y cumplimiento del cargue de los soportes que respalda la ejecución de los controles formulados en las matrices, observaciones, recomendaciones y conclusiones.

Los informes de la Oficina de Control Interno deben contener como mínimo el siguiente contenido: confirmación de la metodología efectuada para el desarrollo del seguimiento, análisis de los resultados obtenidos con base al reporte emitido por la Segunda línea de defensa, evaluación de la estructura y clasificación de los riesgos y controles, evaluación de la ejecución de los controles, seguimiento a la materialización de Riesgos, la formulación de recomendaciones, observaciones y/u oportunidades de mejora aplicables a la gestión del riesgo.

Elaboró: Pablo Molano – Contratista OAP

Revisó: Sindy Tunjano – Contratista OAP

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co