CONCEJO DE MEDELLÍN

Resolución SG 20222100002115
2022-06-22 13:24:34

RESOLUCIÓN SG
20222100002115
2022-06-22

210-16.4

Por medio de la cual se deroga la resolución SG 2015-715 del 28 de diciembre de 2015 y se define la política para la gestión del riesgo del Concejo de Medellín

EL SECRETARIO GENERAL DEL CONCEJO DE MEDELLÍN

En uso de sus facultades legales y administrativas, en especial las conferidas en la Ley 4 de 1992, el artículo 294 del Decreto –Ley 1333 de 1986, el artículo 37 de la Ley 136 de 1994, el Acuerdo Municipal 089 de 2018, y en desarrollo del Decreto 1499 de 2017.

CONSIDERANDO QUE:

Que el Concejo de Medellín cuenta con un Sistema de Gestión Corporativo y se encuentra certificado por el ICONTEC en la NTC ISO 9001: 2015, que en su numeral 6.1 establece como requisito la planificación, ejecución y evaluación de acciones para abordar riesgos y oportunidades

Que el artículo 2.2.22.3.1. del Decreto 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión (MIPG) como una herramienta que integra el Sistema de Gestión de las entidades con su Sistema de Control Interno.

Qué el Modelo Integrado de Planeación y Gestión (MIPG) establece los lineamientos para la gestión del riesgo en la política Transparencia, acceso a la información y lucha contra la corrupción y en la política Control Interno.

Qué el Departamento Administrativo de la Función Pública (DAFP) define lineamientos para la gestión del riesgo en su Guía para la administración del riesgo y el diseño de controles en entidades públicas de octubre de 2018 (versión 4).

Que la Guía para la administración del riesgo y el diseño de controles en entidades públicas de octubre de 2018 (versión 4), establece como primer paso para una adecuada gestión del riesgo, la definición de la Política para la Gestión del Riesgo.

Resolución SG 20222100002115
2022-06-22 13:24:34

Que el Comité Institucional de Gestión y Desempeño establecido mediante Resolución SG 201921000004885 del 17 de septiembre de 2019, como encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión (MIPG), construye y aprueba, en reunión del 17 de mayo de 2022, Acta 19 de 2022, la Política para la Gestión del Riesgo del Concejo de Medellín, siguiendo los lineamientos establecidos en al Guía para la administración del riesgo y el diseño de controles en entidades públicas de octubre de 2018 (versión 4).

RESUELVE

ARTÍCULO PRIMERO. Se adopta la Política para la Gestión del Riesgo aprobada por el Comité Institucional de Gestión y Desempeño en los siguientes términos:

El Concejo de Medellín, para un adecuado manejo de los riesgos asociados a los objetivos estratégicos y a los procesos de la Corporación, implementa la gestión del riesgo como herramienta estratégica que permite disponer de un enfoque preventivo, gestionando los recursos bajo condiciones de eficiencia y eficacia.

A continuación, se definen las condiciones generales para la gestión del riesgo en la Corporación. Se establece los objetivos, el alcance, los niveles para su calificación y aceptación, así como la metodología para el tratamiento de estos. La definición, implementación y el logro de la eficacia de la Política es responsabilidad del Comité Institucional de Gestión y Desempeño – CIG&D del Concejo de Medellín; el seguimiento y evaluación de la implementación de la Política es responsabilidad del Comité Institucional de Coordinación de Control Interno - CICCI de la Corporación.

ARTÍCULO SEGUNDO. Objetivos. La presente política unifica los lineamientos en los aspectos comunes de la metodología para la administración del riesgo propuesta por el Departamento Administrativo de la Función Pública - DAFP, y fortalece el enfoque preventivo, con el fin de facilitar a los servidores públicos de la Corporación, la identificación y tratamiento de cada uno de los riesgos. Establece los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrenta la Corporación. En este sentido se disponen los siguientes objetivos:

- Suministrar la metodología que permita a la Corporación gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de los procesos, para llevarlos a niveles aceptables.
- Proveer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de servidores públicos en los riesgos operativos, de corrupción y de seguridad y privacidad de la información.

- Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan al CIG&D de la Corporación tener una seguridad razonable en el logro de sus objetivos.

ARTÍCULO TERCERO. Alcance La administración de los riesgos es extensible y aplicable a todos los procesos de la Corporación. Para el caso de los Riesgos de corrupción, se adopta la metodología orientada por el Departamento administrativo de la función pública – DAFP, en su Guía para la gestión de riesgos de corrupción.

ARTÍCULO CUARTO. Niveles de aceptación del riesgo. La aceptación de los riesgos dependerá del nivel de afectación que estos tengan en la prestación del servicio y el impacto en los recursos.

De acuerdo con los criterios para el tratamiento de riesgos definidos por el DAFP (Aceptar, Evitar, Reducir o Compartir), se establecen a continuación los niveles de aceptación a los riesgos.

Nivel de riesgo inherente:

Nivel Bajo: se ACEPTARÁ el riesgo y no se realizará la valoración de controles para el mismo; su control y registro de avance se realizará trimestralmente por medio del reporte de la gestión del riesgo.

Para el resto de los niveles (Medio, Alto, Extremo): Se identificarán controles que permitan REDUCIR la probabilidad de ocurrencia y/o el impacto del riesgo; se realizará seguimiento trimestral a la aplicación de dichos controles y se registrarán sus avances en el reporte de la gestión del riesgo.

Nivel de riesgo residual

Nivel Bajo: se ACEPTARÁ el riesgo y administrará por medio de las actividades propias del proceso asociado; su control y registro de avance se realizará trimestralmente por medio del reporte de la gestión del riesgo.

Para el resto de los niveles (Medio, Alto, Extremo): Se establecerán acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo; se realizará seguimiento trimestral a la aplicación de dichos controles y se registrarán sus avances en el reporte de la gestión del riesgo.

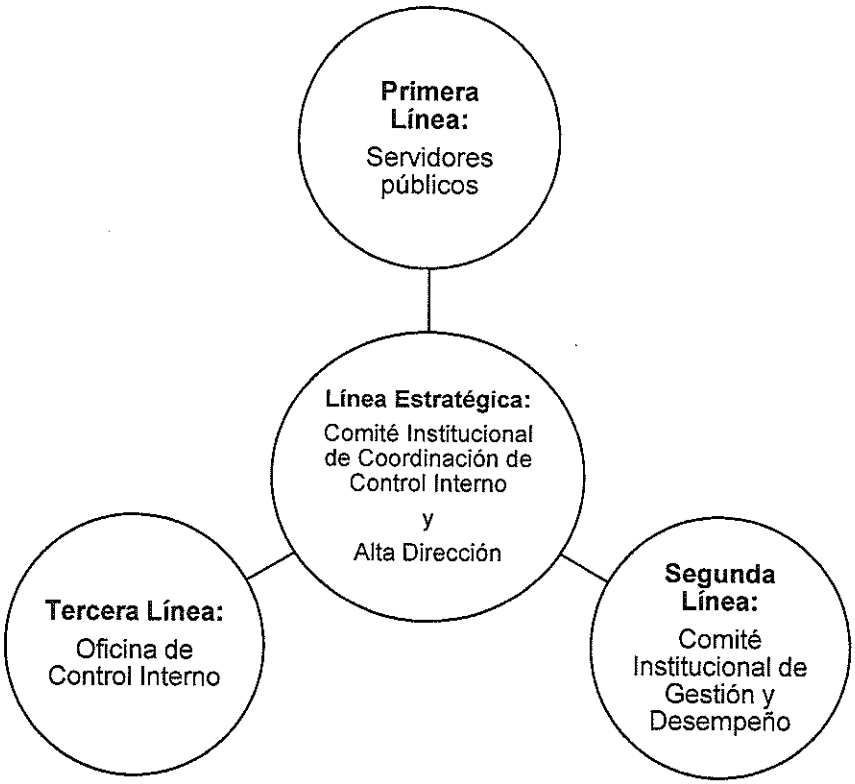
Dependiendo de la naturaleza del riesgo (factores de riesgo) es posible que algunos clasificados en nivel extremo puedan COMPARTIRSE o EVITARSE, previo análisis en el Comité Institucional de Coordinación de Control Interno.

Lo anterior se considera en el Instructivo para la identificación, análisis y evaluación, de riesgos (I-GEP-016).

Es importante considerar que los riesgos de corrupción **no admiten aceptación del riesgo**, siempre deben conducir a un tratamiento.

ARTÍCULO QUINTO. Niveles para calificar el impacto. El análisis varía de acuerdo con la complejidad de cada uno de los riesgos, para el efecto será necesario considerar el proceso al cual pertenece y el tipo de riesgo (riesgo de servicio, de talento humano, físicos, de capacidad financiera, entre otros aspectos). Los niveles y el impacto se definen en el en el numeral 3.1 Análisis de riesgos de la Guía para la administración del riesgo y la definición de controles del Departamento Administrativo de la función pública (versión 4, 2018).

ARTÍCULO SEXTO. Líneas de defensa. Las líneas de defensa identificadas para el Concejo de Medellín son:



Fuente: *Adoptado del Manual Operativo de MIPG V4, 2021.*

ARTÍCULO SÉPTIMO. Reporte de las líneas de defensa. Para cada línea de defensa se definen los siguientes temas a reportar y la periodicidad de presentación de los reportes:

Primera Línea.

Temas a reportar:

- Riesgos materializados que identifiquen en su labor diaria, mediante correo electrónico a su superior inmediato.
  Periodicidad: cuando ocurra la materialización del riesgo.

- Alertas sobre posibles situaciones que generen riesgos, mediante correo electrónico a su superior inmediato.
  Periodicidad: cuando se presente la situación.

- Deficiencias que se identifican en el diseño y aplicación de los controles definidos para los riesgos, mediante correo electrónico a su superior inmediato.
  Periodicidad: cuando se identifique la situación.

Uno de los temas tratados en grupo primario será la gestión de los riesgos del respectivo proceso.

Segunda Línea.

Temas a reportar:

- Análisis realizados a los riesgos materializados identificados y planes de mejora definidos.
  Periodicidad: CIG&D de seguimiento trimestral.

- Cambios propuestos en la definición de riesgos y en el diseño y ejecución de los controles.
  Periodicidad: CIG&D de seguimiento trimestral.

- Propuestas de nuevos riesgos identificados.
  Periodicidad: CIG&D de seguimiento trimestral.

En enero de la vigencia siguiente, se genera un informe anual de seguimiento a la gestión del riesgo considerando los reportes presentados en las reuniones de seguimiento trimestral del CIG&D, y se analiza dicho informe en el Comité Institucional de Coordinación de Control Interno.

Tercera Línea.

Tema a reportar: análisis consolidado de los hallazgos o situaciones irregulares identificado en los informes generados por la Oficina de Control Interno.

Periodicidad de reporte: trimestralmente en Comité Institucional Coordinación de Control Interno (Línea Estratégica).

ARTÍCULO OCTAVO. Lineamientos para la gestión del riesgo en la Corporación. Se establecen las siguientes directrices generales para una adecuada gestión del riesgo en el Concejo de Medellín:

Identificación del riesgo.

La identificación del riesgo es el punto de partida para una adecuada Gestión del Riesgo. Se deben considerar:

- La fuente del riesgo (objetivos estratégicos, proceso del Sistema de Gestión Corporativo).
- El contexto interno, externo y del proceso que pueden afectar el logro de los objetivos.

A partir de la identificación de la fuente y del análisis del contexto, se determina:

- Las causas de riesgo.
- El riesgo y su descripción.
- La clasificación para definir el tipo de riesgo (estratégico, gerencial, operativo, etc.).
- Los efectos más probables que pueden generar la materialización del riesgo.

Establecimiento del contexto.

Para realizar la identificación del riesgo se realiza la definición de los parámetros internos, externos y del proceso que se han de tomar en consideración para la definición de las causas de los riesgos a identificar. Se pueden considerar los siguientes factores asociados a cada categoría del contexto:

Tabla 1. *Factores a analizar por cada contexto.*

CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información, externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos generados.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	ECONÓMICOS: presupuesto de funcionamiento, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.

	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Probabilidad e Impacto.

Para determinar la probabilidad de ocurrencia y el nivel del impacto del riesgo se siguen los lineamientos del Instructivo para la identificación, análisis y evaluación, de riesgos (I-GEP-016) y se consideran las tablas de probabilidad e impacto definidas en el numeral 3.1 Análisis de riesgos de la Guía para la administración del riesgo y la definición de controles del Departamento Administrativo de la función pública (versión 4, 2018).

Para determinar la probabilidad se debe seleccionar de las opciones la probabilidad de materialización del riesgo, siendo 1: Poco probable y 5: Muy probable.

Para la clasificación del impacto se debe seleccionar de las opciones, los impactos o consecuencias que puede llegar a traer la materialización del riesgo previamente identificado.

Controles.

Se definen los controles para prevenir o disminuir el impacto o probabilidad de los riesgos identificados, y seguidamente se califican dichos controles respecto a su diseño y ejecución, considerando los criterios definidos en la Guía para la administración del riesgo y la definición de controles del Departamento Administrativo de la función pública (versión 4, 2018).

Los criterios de evaluación para calificar el diseño de los controles consideran: la asignación de un responsable, la pertinencia de ese responsable, la periodicidad de ejecución del control, el propósito y confiabilidad del control, el tratamiento al control que falla y las evidencias de ejecución del control.

La calificación de la ejecución del control se realiza con base en la frecuencia con la que se utiliza el mismo.

Responsabilidades frente a los riesgos de seguridad y privacidad de la información.

El responsable de seguridad digital y seguridad de la información en la Corporación se encarga de:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Periodicidad de monitoreo y revisión de los riesgos.

El monitoreo es constante por la primera y tercera línea de defensa, el análisis y la revisión se hace cada trimestre en el marco del Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno; además se define el siguiente tratamiento:

- Anualmente, en el **Comité Institucional de Gestión y Desempeño** se revisa el mapa de riesgos de la Corporación, para lo cual se tomará como insumo, las auditorías, evaluaciones y los planes de mejora por proceso relacionados con la gestión de los riesgos.

- El análisis se realiza trimestralmente, posterior al cierre de cada trimestre a iniciarse en el mes de enero, donde se debe entregar por parte de los Líderes de proceso el informe de gestión de riesgos con los resultados del periodo.

- Previa coordinación con los Líderes de proceso, y de manera periódica, la tercera línea de defensa monitora los riesgos que se encuentran en la zona de mayor impacto, con el fin de evidenciar si se materializó alguno de ellos, y si es necesario ajustar o considerar nuevos controles.

ARTÍCULO NOVENO. Metodología. Para la Corporación es importante definir otros aspectos que la misma considere necesarios, con el fin de generar orientaciones claras y precisas para todos los servidores públicos, de tal modo que la gestión del riesgo sea efectiva y esté articulada con la estrategia de la Corporación. Para el efecto se dispone del Procedimiento para la gestión del riesgo (P-GEP-002).

ARTÍCULO DÉCIMO. Derogar en su integridad la Resolución SG2015-275 del 28 de diciembre de 2015.

La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

CONRADO DE JESÚS TORRES GRACIANO
Secretario General Encargado

Proyectó: Juanita Guevara Hurtado
Radicó: Maria Isabel Correa Restrepo