INTERNO
CONSECUTIVO No. 0 0 0 1 5 3

CONCEJO DE BELLO
Una decisión para todos

2 2 MAR 2024

HORA: 10:55

FIRMA:

RESOLUCIÓN No. 058
CONCEJO MUNICIPAL DE BELLO
(22 de marzo de 2024)

"POR MEDIO DE LA CUAL ACTUALIZA Y ADOPTA LA POLÍTICA DE RIESGO DEL CONCEJO MUNICIPAL DE BELLO".

El Presidente del Concejo Municipal de Bello Antioquia, en uso de sus facultades y en especial las conferidas por la Ley 136 de 1994; La Ley 152 de 1994 de 2011, Ley 87 De 1993, Ley 1474 De 2011 y,

CONSIDERANDO:

1. Que mediante la Resolución N°024 de 30 de enero de 2024, el Concejo Municipal de Bello adopto el Plan Estratégico Corporativo para el periodo 2024-2027.

2. Que la planeación se constituye en el instrumento de gestión fundamental para orientar el cumplimiento de la Visión y Misión de la Corporación, mediante el establecimiento de objetivos y metas para ejecutar durante el periodo administrativos.

3. Que el Decreto 1083 de 2015, modificado por los Decreto 648 y 1499 de 2017 establecen que "El Sistema de Gestión, creado en el artículo 133 de la Ley 753 de 2015, que integra los Sistemas de Desarrollo Administrativo y de Gestión de la institucional y a la consecución necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad. ", y se dispone además que 'Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo."

4. Que la Ley 87 de 1993, establece el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones; Articulo 2. Literal f) Definir y aplicar medidas para prevenir la materialización de los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos"

5. Que la administración del riesgo es un componente del Direccionamiento Estratégico, el cual obliga a las entidades públicas a emprender las acciones necesarias que le permitan el manejo de eventos (riesgos) que puedan afectar el logro de los objetivos institucionales. Para lo cual se deben integrar los elementos constitutivos el contexto estratégico; la identificación de riesgos; el análisis de riesgos; la valoración de riesgos y políticas de administración del riesgo. Todos

estos elementos conducen a la definición de criterios básicos en la formulación del estándar de control que se consolida en las políticas de administración de riesgos.

6. Que con la expedición del 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", se realizó la articulación entre el Modelo Integrado de Planeación y Gestión MIPG y el Sistema de Control Interno.

7. Que el artículo 73 de la Ley 1474 de 2011 modificado por el artículo 31 de la Ley 2195 de 2022 establece que "Cada entidad del orden nacional, departamental y municipal cualquiera que sea su régimen de contratación, deberá implementar Programas de Transparencia y Ética Pública con el fin de promover la cultura de la legalidad e identificar, medir, controlar y monitorear constantemente el riesgo de corrupción en el desarrollo de su misionalidad.

8. Que la Norma ISO 31000:2018 es un estándar de origen internacional que ha sido desarrollado por ISO, y que proporciona los principios y directrices para la Gestión de Riesgos. Al igual que el resto de las normas ISO, es aplicable a cualquier tipo de organización, independientemente del sector, tamaño o actividad que realice; y es allí donde se establecen disposiciones que ayudan al diseño, implementación, operación, mantenimiento y revisión de un sistema de Gestión de Riesgos basado en la mejora continua.

9. Que el Departamento Administrativo de la Función Pública - DAFP emitió la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6, de noviembre de 2022, por lo que se hace necesario actualizar la Política de Administración del Riesgo

RESUELVE

ARTÍCULO PRIMERO: Actualizar, adoptar y desarrollar la Política de Administración de Riesgos para el Concejo Municipal de Bello, la cual hace parte integral de la presente Resolución, a través del adecuado tratamiento de los riesgos de gestión institucional por planes, programas, proyectos y procesos y que incluya los asociados a: activos seguridad de la información; seguridad y salud ocupacional, y los posibles riesgos relacionados con eventos de corrupción, para garantizar el cumplimiento de la misión, visión y objetivos institucionales, la cual será la base para la definición de los planes de contingencia y continuidad de la entidad; acogiendo la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6, de noviembre de 2022, emitida por el Departamento Administrativo de la Función Pública DAFP.

ARTÍCULO SEGUNDO: En el marco de los Sistemas de Gestión se deben estructurar criterios orientadores en la toma de decisiones, respecto al tratamiento de los riesgos y sus efectos al interior de la Corporación. Por tanto, la implementación de la Política de Administración de Riesgos estará coordinada por la Alta Dirección de los Sistemas de Gestión, el equipo directivo y con el apoyo del equipo operativo: también debe ser interiorizada por todos los servidores públicos y contratistas que sean responsables y/o

participen en el desarrollo de los diferentes planes, programas, proyectos y/o de los procesos de selección o contratación. los riesgos estarán articulados con las políticas de transparencia, acceso la información pública y lucha contra la corrupción de la Corporación.

ARTICULO TERCERO: El ordenador del gasto del Concejo Municipal de Bello suministrará los recursos necesarios pala la efectiva aplicación de los controles determinados para cada uno de los riesgos establecidos en el mapa de riesgos institucional.

ARTICULO CUARTO: Para la implementación de la Política de Administración del Riesgo, el Concejo Municipal de Bello, se basará en los análisis de las estrategias, la formulación de objetivos y la implementación de esos objetivos en la toma de decisiones, aspectos fundamentales frente a la generación de valor público eje fundamental en el quehacer de la Entidad pública.

ARTÍCULO QUINTO: Derogar en todas sus partes de Política de Riesgo adoptada mediante la Resolución N°148 del 05 de septiembre de 2022 para el Concejo Municipal de Bello.

ARTICULO SEXTO: La presente Resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que sean contrarias.

Dada en el Municipio de Bello, a los veintidós (22) días del mes de marzo de dos mil veinticuatro (2024).

DANIEL RODRIGO VILLA MALDONADO
Presidente Concejo de Bello

Aprobó: Comité Institucional de Gestión y Desempeño

Revisó: Jose Argemiro Restrepo Restrepo, Jefe ~~de Oficina Asesora~~ Jurídica

Proyectó: Paola Andrea Vélez Monsalve – P.U. Planeación y Presupuesto Paola Vélez
GHA Londoño y Ossa S.A.S.

POLITICA Y GUÍA DE ADMINISTRACIÓN DE RIESGOS

CONCEJO MUNICIPAL DE BELLO- ANTIOQUIA

Febrero de 2024

INTRODUCCIÓN

El Concejo Municipal de Bello actualiza su Política de Riesgos conforme a los lineamientos establecidos por el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno MECI y las líneas de defensa, los referentes de la Guía para la Administración del riesgo emitida por el Departamento Administrativo de la Función Pública – DAFP -, el diseño de controles y los demás lineamientos expedidos por los entes rectores referentes a la Administración del Riesgo.

El presente documento determina las políticas de operación en cuanto a la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y los efectos que puede ocasionar su materialización con el fin de blindar la misión y objetivos institucionales, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, planes, programas y proyectos institucionales.

La Corporación a través de la adecuada administración de los riesgos orientará su gestión al mejoramiento continuo del control y de la gestión del Concejo Municipal, así como de su capacidad para responder efectivamente a las expectativas y necesidades de las partes interesadas.

Los lineamientos establecidos en esta política son de obligatorio cumplimiento para los actores que intervienen en el cumplimiento de la misión del Concejo Municipal y los objetivos establecidos en los procesos estratégicos.

MARCO NORMATIVO

El Decreto 1081 de 2015 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República", reglamentario de los artículos 73 y 76 de la Ley 1474 de 2011.

La Ley 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" ***ARTÍCULO 31. PROGRAMAS DE TRANSPARENCIA Y ETICA EN EL SECTOR PUBLICO, el cual modifica el artículo*** *73 de la Ley 1474 de 2011*

Con la expedición del 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", se realizó la articulación entre el Modelo Integrado de Planeación y Gestión MIPG y el Sistema de Control Interno.

Decreto 1072 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo.

Resolución 0312 de 2019, por la cual se definen los estándares mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST.

Norma Técnica Colombiana ISO 9001:2015 Sistema de Gestión de la Calidad.

Norma Técnica Colombiana ISO 31000:2018 Gestión del Riesgo.

Norma Técnica Colombiana ISO/IEC 27001:2022 "Sistema de Gestión de la Seguridad de la Información".

Norma Técnica Colombiana ISO 27005:2018 "Seguridad de la información y las comunicaciones".

Norma Técnica de Colombiana ISO 45001:2015 "Sistema de Gestión de Seguridad y Salud en el Trabajo".

TÉRMINOS Y DEFINICIONES:

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales

- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias:

- **Riesgos Estratégicos**: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

- **Riesgos Gerenciales**: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

- **Riesgos Operativos**: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

- **Riesgos Financieros**: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

- **Riesgos Tecnológicos**: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una Entidad.

- **Riesgos de Cumplimiento**: Posibilidad de ocurrencia de eventos que afecten la situación jurídica y contractual de la entidad, debido a su incumplimiento o desacato a la normatividad legal o las obligaciones contractuales.

- **Riesgo de Imagen o de Reputación**: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

- **Riesgo de corrupción: Posibilidad** de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Riesgo inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

- **Probabilidad**: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Gestión del Riesgo**: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la Administración un aseguramiento razonable con respecto al logro de los objetivos.

- **Impacto**: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Control:** Medida que permite reducir o mitigar un riesgo.

- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.

- **Programa de Transparencia y Ética Pública:** Promover la cultura de la legalidad e identificar, medir, controlar y monitorear constantemente el riesgo de corrupción en el desarrollo de su misionalidad.

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **Confidencialidad**: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

- **Control**: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

- **Amenazas**: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una entidad.

- **Integridad**: Propiedad de exactitud y completitud.

- **Disponibilidad**: Propiedad de ser accesible y utilizable a demanda por una entidad

- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.

- **Tolerancia al riesgo**: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- **Apetito al riesgo**: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Contingencia**: Posible evento futuro, condición o eventualidad

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

- **Restablecimiento:** Capacidad de la entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Concejo Municipal de Bello se compromete a gestionar continuamente los riesgos que puedan afectar los planes estratégicos de la Corporación derivados de factores internos o externos, mediante la identificación, análisis y valoración de riesgos, así como el establecimiento de los controles y acciones de tratamiento para los riesgos de mayor impacto y probabilidad, que permitan prevenir la ocurrencia de las situaciones de riesgos o mitigar los efectos de tales riesgos; procurando promover la cultura de la legalidad e identificar, medir, controlar y monitorear constantemente el riesgo de corrupción en el desarrollo de su misionalidad en cumplimiento del Programa de Transparencia y Ética Pública.

OBJETIVOS DE LA POLITICA DE ADMINISTRACIÓN DE RIESGOS

Establecer los lineamientos para el tratamiento, manejo y seguimiento de los riesgos que afecten el logro de los objetivos institucionales del Concejo Municipal de Bello, a través de la identificación, valoración, tratamiento, manejo y seguimiento a los riesgos de gestión, corrupción, seguridad de la información y seguridad y salud en el trabajo, con el fin de mitigar o eliminar sus efectos.

OBJETIVOS ESPECÍFICOS:

- Implementar una herramienta metodológica para la gestión de los diferentes tipos de riesgos en todos los procesos de la Corporación.
- Socializar la política de Administración de riesgos a las partes interesadas.
- Definir los roles y responsabilidades frente a la gestión de los riesgos en la entidad.
- Identificar los riesgos de gestión, corrupción, y de seguridad de la información del Concejo Municipal de Bello.
- Disminuir la probabilidad e impacto de materialización de los riesgos en la Corporación
- Generar mecanismos para tratar las amenazas y vulnerabilidades que enfrentan los activos e información y de tecnología, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información de la entidad.

ALCANCE:

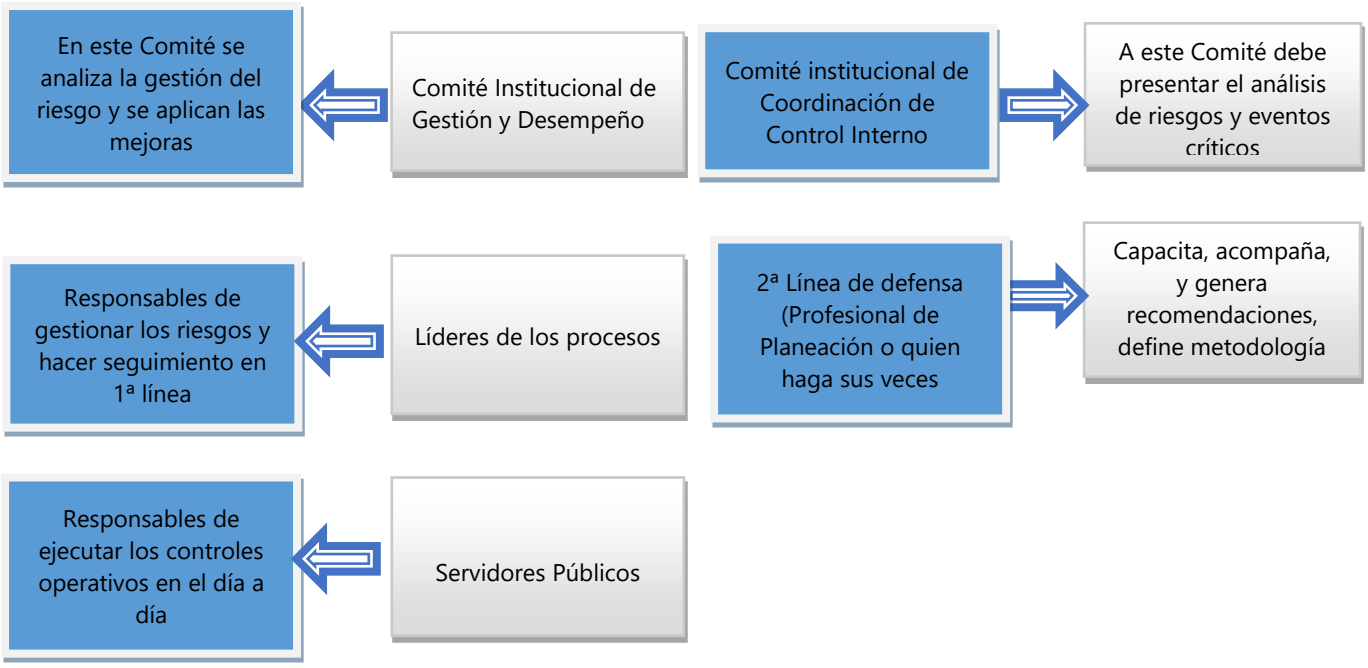
La política de Administración de riesgos es aplicable a todos los procesos del Concejo Municipal de Bello en el desarrollo de las actividades descritas en la cadena de valor y las acciones permanentes que desarrollan los funcionarios en cumplimiento de los objetivos estratégicos.

Institucionalidad

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:

Operatividad institucional para la gestión del riesgo



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

ROLES Y RESPONSABILIDADES

Líneas de Defensa	Responsables	Responsabilidad frente al riesgo
Línea estratégica	Presidente Comité de Gestión y Desempeño Institucional. Comité Institucional de Control Interno.	- Definir y aprobar el marco general para la gestión del riesgo, la gestión de la continuidad y el control. - Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad institucional que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. - Definir y aprobar la política para la Administración del riesgo. - Garantizar el cumplimiento de los planes de la entidad.

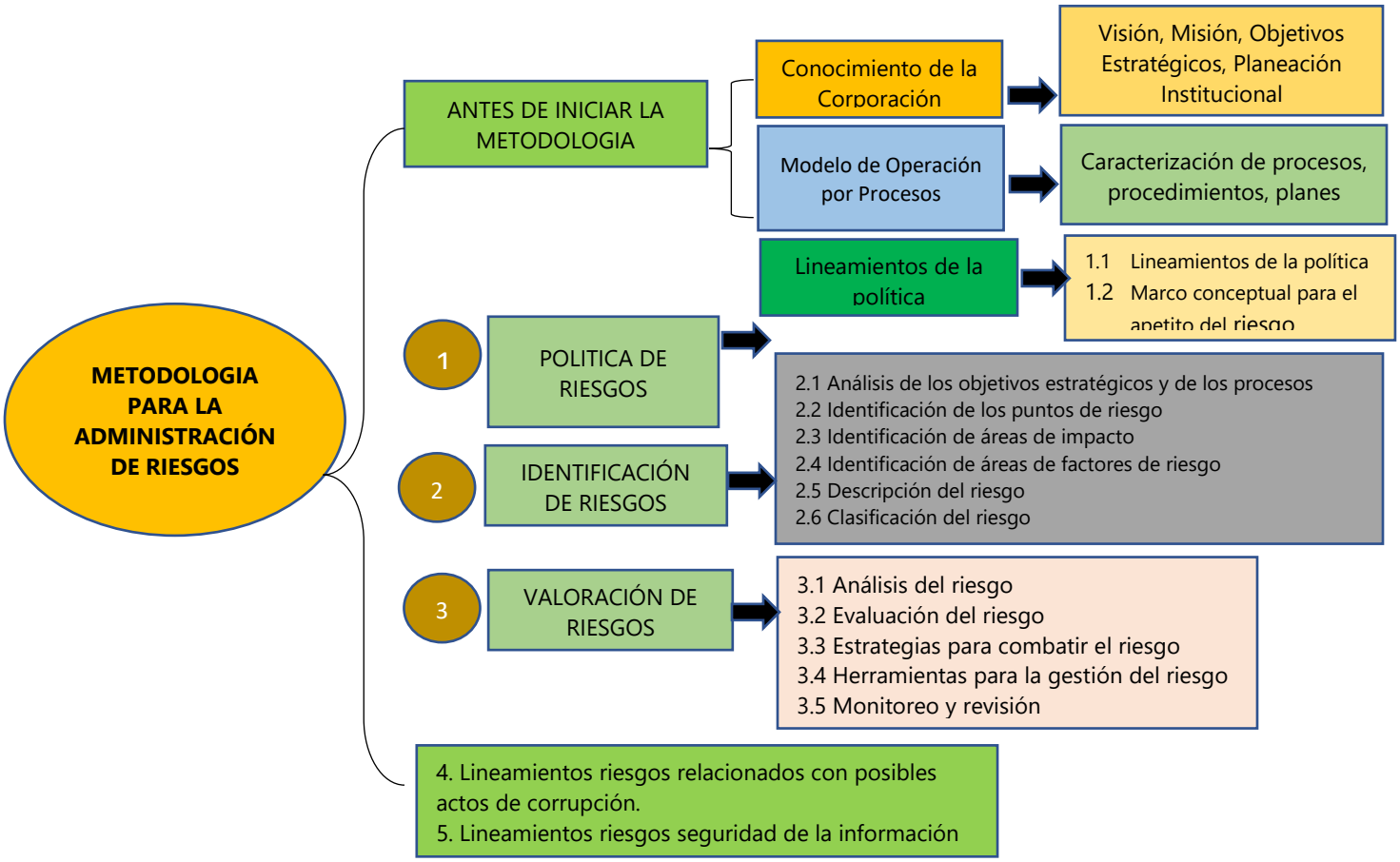
Líneas de Defensa	Responsables	Responsabilidad frente al riesgo
Primera línea de defensa	Presidente Secretaría General Jefe de Oficina Jurídica y Contratación Administrativa Jefe de Oficina de Talento Humano y Asuntos Disciplinarios	- Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso. - Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. - Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. - Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad. - Informar a la Secretaría General y Profesional de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. - Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
Segunda Línea de Defensa	Secretaría General Profesional de Planeación	- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. - Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. - Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. - Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. - Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.

Líneas de Defensa	Responsables	Responsabilidad frente al riesgo
		- Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación. - Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad bajo su responsabilidad. - Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y las estrategias de continuidad asociadas a los escenarios de continuidad bajo su responsabilidad y los temas a su cargo. - Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. - Realizar el seguimiento al mapa de riesgos de su proceso. - Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. - Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad en los temas de su competencia. - Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
Tercera línea de defensa	Oficina de Control Interno de Gestión	- Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. - Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa - Asesorar a la primera línea de defensa de forma coordinada con la Secretaría General y Profesional de Planeación, en la identificación de los riesgos y diseño de controles. - Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad operativa consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados. - Recomendar mejoras a la política de

Líneas de Defensa	Responsables	Responsabilidad frente al riesgo
		operación para la Administración del riesgo.

METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO:

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada



Marco conceptual para el apetito del riesgo:

Teniendo en cuenta que dentro de los lineamientos para la política de Administración del riesgo se debe considerar el apetito del riesgo, a continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis en el Concejo Municipal de Bello, iniciando con las siguientes definiciones:

- **Nivel de riesgo:** es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Tolerancia del riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Determinación de la capacidad de riesgo

La entidad debe aplicar los valores de probabilidad e impacto contenidos en esta Guía y con base en esto debe determinar, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.

b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina "capacidad de riesgo".

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que la entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

Determinación del apetito de riesgo

Luego de determinada la capacidad de riesgo por parte de la Alta Dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.

Este valor se denomina "apetito de riesgo", dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Tolerancia de riesgo

La tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

Identificación del riesgo

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Se aplican las siguientes fases:

1. **Análisis de objetivos estratégicos y de los procesos:** este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

2. **Identificación de los puntos de riesgo:** son 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.

3. **Identificación de áreas de impacto:** el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

4. **Identificación de áreas de factores de riesgo:** son las fuentes generadoras de riesgos.

Tabla: Factores de riesgo

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la entidad.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento Humano	Se analiza posible dolo e intención frente a la corrupción.	Hurto de activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
		Suplantación de identidad

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Evento externo	Situaciones externas que afectan la entidad.	Asalto a la oficina
		Atentados, vandalismo, orden público

1. **Descripción del riesgo**: La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Estructura para la redacción del riesgo

Esta estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- **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 sub-causas que pueden ser analizadas.

- **Clasificación del riesgo:** Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Clasificación de riesgos

Ejecución y Administración de procesos	Pérdidas derivadas de errores en la ejecución y Administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	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.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

VALORACIÓN DEL RIESGO

En esta etapa se establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

1. **Análisis de riesgos:** en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

2. **Determinar la probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo.

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Criterios para definir el nivel de probabilidad

	Frecuencia de la actividad	Probabilidad
Muy baja	Actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5000 por año	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

3. Determinar el impacto:

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Criterios para definir el nivel de impacto

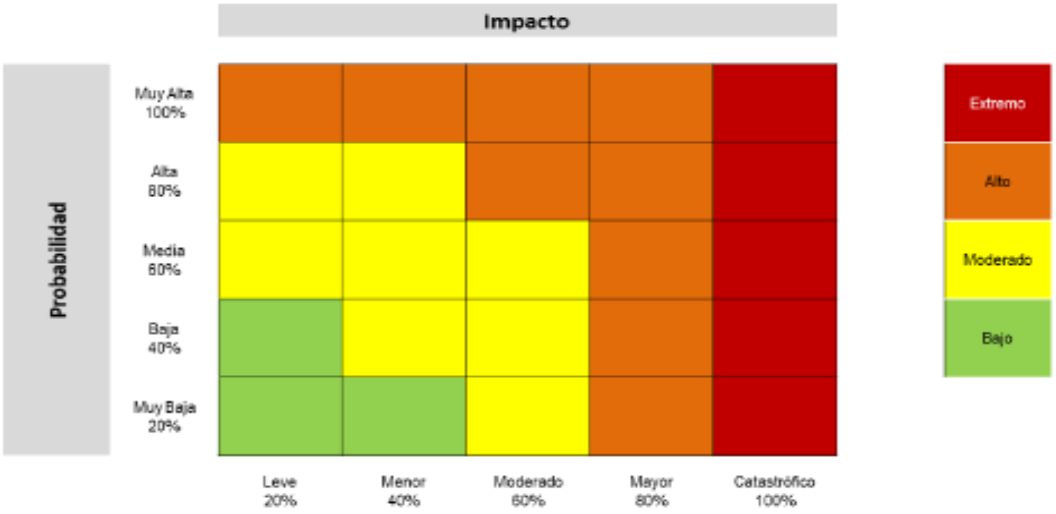
Nivel	Afectación económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la entidad.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general a nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Evaluación de Riesgos:

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).

1. **Análisis preliminar (riesgo inherente):** Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Matriz de calor (niveles de severidad del riesgo)



1. **Valoración de controles:** Un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer.

- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Tipología de controles y los procesos: A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión.

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

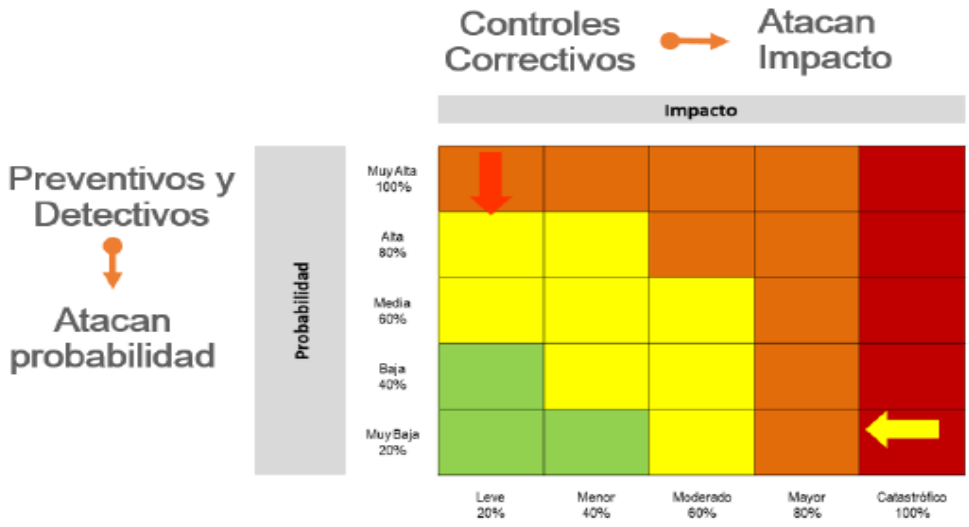
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Atributos para el diseño del control

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Correctivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Detectivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
Atributos de eficiencia	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos Informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
			Identifica a los controles que pese a que se ejecutan en el proceso no se	

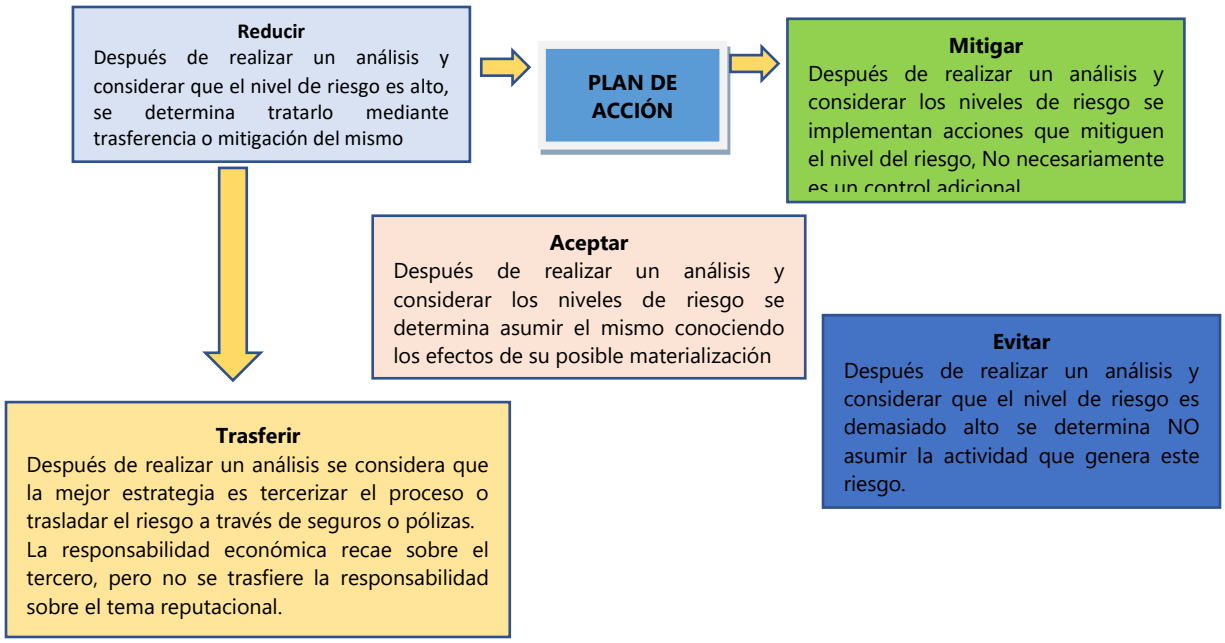
Características			Descripción	Peso
		Sin documentar	encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	-
	Evidencia	Con registro	El control deja un registro, permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

NOTA: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.



Estrategias para combatir el riesgo: Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.



Herramientas para la gestión del riesgo: como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

1. Gestión de eventos: Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, 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.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia

Riesgos Seguridad de la Información:

Para el caso de los riesgos sobre seguridad de la información, para el Concejo Municipal, se ha definido la incorporación del Anexo 4 Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en entidades públicas, de manera tal que los responsables analicen y establezcan, en el marco de sus procesos, los activos de información asociados y se identifiquen los riesgos correspondientes. En cuanto a los riesgos de seguridad de la información se incorporan las tablas de probabilidad, impacto y matriz de calor definidas en la metodología general.

Los riesgos de seguridad de la información se basan en la afectación de tres criterios en un activo de información o un grupo de activos de información dentro del proceso: "Integridad, confidencialidad o disponibilidad" Solo existen tres (3) tipos de riesgos:

- Pérdida de confidencialidad,
- Pérdida de la integridad
- Pérdida de la disponibilidad de los activos de información.

Para cada tipo de riesgo se seleccionarán las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice. Para el riesgo identificado se deben asociar el grupo de activos de información o activos de información específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Riesgos de corrupción:

Para los riesgos asociados a posibles actos de corrupción se han definido los lineamientos para su tratamiento. Es claro que este tipo de riesgos no admiten aceptación del riesgo; así mismo, se han incluido las matrices relacionadas con la redacción de este tipo de riesgos, las preguntas para la definición del nivel de impacto y la matriz de calor correspondiente, donde se precisan las zonas de severidad aplicables. Para esta tipología de riesgos se incluye el protocolo para la identificación de riesgos de corrupción, asociados a la prestación de trámites y servicios, en el marco de la política de racionalización de trámites, en los casos que aplique.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ DEFINICIÓN DE RIESGOS DE CORRUPCIÓN				
Descripción del Riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	**X**	**X**	**X**	**X**

Medición de impacto de riesgos de Corrupción.

La medición del impacto de los riesgos de corrupción se realizará aplicando la siguiente tabla de valoración. Cada riesgo identificado es valorado de acuerdo con las preguntas la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Criterios para calificar el impacto en los riesgos de corrupción

N	Pregunta ¿Si el riesgo se materializa podría?	Respuesta Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al cual pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida de los bienes o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen Nacional?		
19	¿Generar daño ambiental?		

Criterios para calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Medición de impacto de riesgo de corrupción			
Descriptor	**Descripción**	**Nivel**	**Respuestas afirmativas**
Moderado	Afectación parcial al proceso y a la dependencia Genera medianas consecuencias para la entidad	5	1-5
Mayor	Impacto negativo de la entidad Genera altas consecuencias para la entidad	10	6-11
Catastrófico	Consecuencias desastrosas para el sector Genera consecuencias desastrosas para la entidad	20	12-16

Estrategias para la aceptación del riesgo residual

Acorde con los riesgos residuales aprobados por el Comité Institucional de Coordinación de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados, así:

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	ESTRATEGIA DE TRATAMIENTO
Riesgos de Gestión y Seguridad de la información	Baja	Se **ACEPTA** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte trimestral de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad o el impacto de

		ocurrencia del riesgo, se hace seguimiento trimestral y se registran sus avances en el mapa de riesgos
	Alta y Extrema	Se establecen acciones de Control Preventivas que permitan **EVITAR** la materialización del riesgo. Se monitorea **MENSUALMENTE** y se registra en el Mapa de riesgos
Riesgos de Corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado. La periodicidad de seguimiento es **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. La periodicidad del seguimiento es **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra en el mapa de riesgos.
	Alta y Extrema	**REDUCIR** la probabilidad, el impacto o ambos factores del riesgo; la estrategia conlleva a la implementación de controles. **EVITAR** Se abandonan o modifican las actividades que dan lugar al riesgo, decidiendo No iniciar, no continuar o modificar de forma segura la actividad que causa el riesgo. **COMPARTIR** con un tercero el tratamiento de una parte del riesgo para reducir la probabilidad, el impacto o ambos factores. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra en el Mapa de riesgos.

Seguimiento a las acciones de control del riesgo en cada proceso

- Según la periodicidad definida para cada riesgo, el líder de riesgos en cada proceso y el líder de este verifica las acciones preventivas y registra el avance junto con la evidencia en el SGI.

- El delegado de riesgo en cada proceso y el líder de este analizan los resultados del seguimiento y establece acciones inmediatas ante cualquier desviación.

- El líder del proceso comunica las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir.

- El líder del proceso verifica que se documenten las acciones de corrección o prevención en el plan de mejoramiento.

- El delegado de riesgo en cada proceso y el líder de este revisa y actualiza, con el acompañamiento del profesional de planeación el mapa de riesgos cuando se modifiquen las acciones o la ubicación del riesgo

Indicadores clave de riesgo: Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

El Concejo Municipal ha definido dos indicadores como mínimo por proceso de la siguiente manera:

Indicador de Eficacia que indique el cumplimiento de las actividades de la gestión del riesgo en cada proceso de la entidad.

EFICACIA

Indicador: Porcentaje de controles implementados = (controles implementados/# de controles definidos) X 100

Indicador de Efectividad para cada riesgo o la suma de todos los riesgos.

EFECTIVIDAD

Indicador: índice de riesgos materializados = (# de riesgos materializados/ total de riesgos identificados) X100

Comunicación y consulta

La comunicación y consulta con las partes involucradas, tanto internas como externas, tendrá lugar durante todas las etapas del proceso para la gestión del riesgo.

BREVE DESCRIPCIÓN DEL CAMBIO	VERSIÓN	FECHA aaaa-mm-dd
No aplica para la primera versión	01	2022-08-02
Ajuste del marco normativo, roles y responsabilidades;	02	2024-02-19

Elaboró	GHA Londoño y Ossa S.A.S, Contratista	Fecha	2024-02-19
Revisó	Paola Andrea Vélez Monsalve	Fecha	2024-02-19
Aprobó	Comité Institucional de Gestión y Desempeño	Fecha	2024-02-28