ALCALDÍA MUNICIPAL DE SAN SEBASTIÁN DE MARIQUITA

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

ALCALDIA MUNICIPAL DE SAN SEBASTIAN DE MARIQUITA

CONTENIDO

1. INTRODUCCION 2

2. Declaración institucional sobre el compromiso frente a la gestión del riesgo 3

3. Marco legal 3

4. Operatividad, institucionalidad para la administración del riesgo 4

5. OBJETIVO 4

6. ALCANCE 5

7. TERMINOS Y DEFINICIONES 5

8. METODOLOGIA 7

9. Niveles de Responsabilidad 10

11. Identificación de Riesgos 15

Valoración del Riesgo 16
Identificación del control y valoración del riesgo residual 20

12. Riesgos fiscales 24

13. Riesgos de seguridad de la información 28

14. Otras disposiciones con relación a la gestión de los riesgos 33

15. Seguimiento al cumplimiento de la política, monitoreo y revisión de los riesgos 34

16. Seguimiento y evaluación del mapa de riesgo 34

17. Comunicación y Socialización de la Política de Gestión del Riesgo 36

1. INTRODUCCION

La política de administración de riesgos de la Alcaldía Municipal de San Sebastián de Mariquita, se define por parte de la Alta Dirección de la entidad a través del Comité Institucional de Coordinación de Control Interno, se implementará con la participación del Comité Institucional de Gestión y Desempeño.

En el presente documento se definen los lineamientos, la metodología a utilizar en la gestión de riesgos, así como de los roles y responsabilidades de acuerdo con las líneas de defensa.

Como instrumento guía para la formulación de la Política de Riesgo se empleó la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, noviembre de 2022, del Departamento Administrativo de la Función Pública.

2. DECLARACIÓN INSTITUCIONAL SOBRE EL COMPROMISO FRENTE A LA GESTIÓN DEL RIESGO

La Alcaldía Municipal de San Sebastián de Mariquita obtiene el compromiso de administrar de forma adecuada los diferentes tipos de riesgos: de gestión, de seguridad de la información, de corrupción, soborno, riesgos fiscales y todas aquellos que puedan afectar el cumplimiento de los objetivos institucionales y por ende la misión de la entidad. Que para ello la entidad garantizará los medios necesarios, apoyo metodológico y el compromiso institucional, teniendo en cuenta que la política se aplicará a todos los procesos desarrollados por la administración.

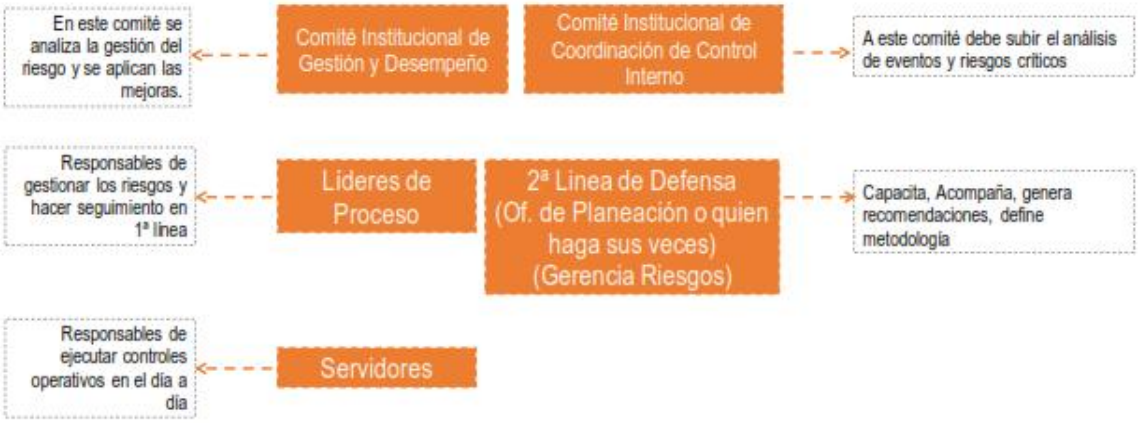
3. MARCO LEGAL

Norma	Expedición	Descripción
Ley 87	1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"
Ley 1474	2011	"Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."
Ley 1712	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.
Ley 1753	2015	por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país", integró en un solo Sistema de Gestión los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, previstos en las Leyes 489 de 1998 y 872 de 2003, respectivamente, el cual deberá articularse con el Sistema de Control Interno consagrado en la Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998.
Manual DAFP	2021	Manual Operativo del Modelo Integrado de Planeación y Gestión Consejo para la Gestión y Desempeño Institucional - versión 4 – marzo 2021
DECRETO 1499	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
Guía DAFP	2022	Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6 - noviembre de 2022
Ley No. 2195	2022	Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.

Decreto 1122	2024	Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública

4. OPERATIVIDAD, INSTITUCIONALIDAD PARA LA ADMINISTRACIÓN DEL RIESGO

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 adecuado gestión del riesgo. Que de acuerdo con lo dicho por la función pública entra a operar de la siguiente forma.



5. OBJETIVO

Definir los lineamientos de la política integral de gestión del riesgo en el municipio de San Sebastián de Mariquita Tolima, que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir en el cumplimiento de sus funciones y objetivos estratégicos institucionales, con el propósito de gestionar los riesgos identificados que permita a la entidad contar con un enfoque preventivo para la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a los ciudadanos del municipio de Mariquita Tolima.

6. ALCANCE

La política de riesgo será aplicable a todos los niveles, nueve (9) procesos misionales, seis (6) procesos de apoyo, al proceso de gestión estratégica, comunicación y de calidad, y al proceso de evaluación y control.

7. TERMINOS Y DEFINICIONES

- **Riesgo**: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **Riesgo Fiscal:** Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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

- **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**.**

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

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

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

- **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.

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

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

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

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

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

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

- **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.

- **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. En general la fórmula del Nivel del Riesgo puede ser Probabilidad por Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **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 se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

- **Apetito de 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**.**

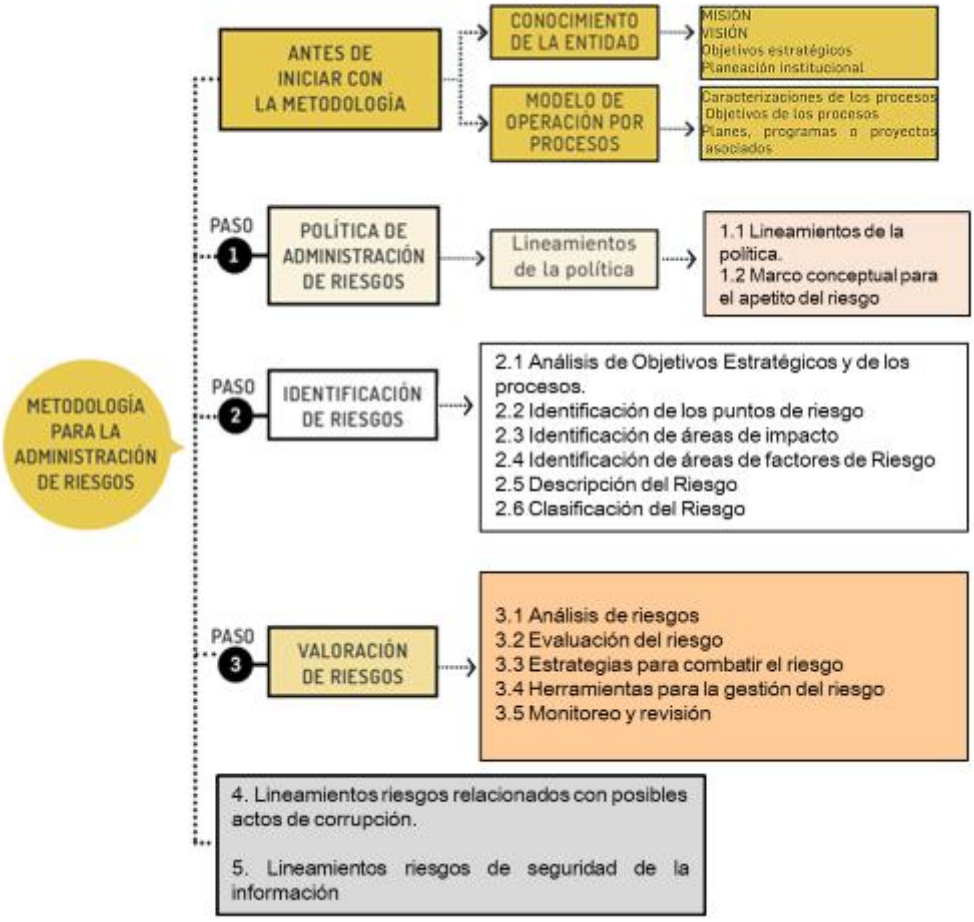
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal, modificado por el artículo 35 de la Ley 2195 de 2022 que establece los Programas de Transparencia y Ética Pública.

8. METODOLOGIA

La administración de riesgos en la alcaldía municipal de San Sebastián de Mariquita, se realizará con base en la Guía de Administración de riesgos del DAFP, versión 6, Esta metodología contempla identificar los riesgos, definir los controles, valoración y finalmente la formulación del Plan de Acción, cuando corresponda, así como el seguimiento a las acciones planeadas. Así mismo Se utilizará la metodología vigente por Colombia Compra Eficiente, para la administración de riesgos para el proceso de contratación dirigido a los partícipes del sistema de compras y contratación pública.

De acuerdo a lo dicho en la Guía de Administración del Riesgo "*la metodología 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 transversal es a toda la entidad para que su efectividad pueda ser evidenciada".*

A continuación estructura completa de sus desarrollo básicos.


METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS
ANTES DE INICIAR CON LA METODOLOGÍA
CONOCIMIENTO DE LA ENTIDAD
MISIÓN
VISIÓN
Objetivos estratégicos
Planeación institucional
MODELO DE OPERACIÓN POR PROCESOS
Caracterizaciones de los procesos
Objetivos de los procesos
Planes, programas o proyectos asociados
PASO 1
POLÍTICA DE ADMINISTRACIÓN DE RIESGOS
Lineamientos de la política
1.1 Lineamientos de la política.
1.2 Marco conceptual para el apetito del riesgo
PASO 2
IDENTIFICACIÓN DE RIESGOS
2.1 Análisis de Objetivos Estratégicos y de los procesos.
2.2 Identificación de los puntos de riesgo
2.3 Identificación de áreas de impacto
2.4 Identificación de áreas de factores de Riesgo
2.5 Descripción del Riesgo
2.6 Clasificación del Riesgo
PASO 3
VALORACIÓN DE RIESGOS
3.1 Análisis de riesgos
3.2 Evaluación del riesgo
3.3 Estrategias para combatir el riesgo
3.4 Herramientas para la gestión del riesgo
3.5 Monitoreo y revisión
4. Lineamientos riesgos relacionados con posibles actos de corrupción.
5. Lineamientos riesgos de seguridad de la información

FUENTE DAFP

9. NIVELES DE RESPONSABILIDAD

A través de la siguiente matriz se definen la responsabilidad frente al riesgo, acorde con las líneas de defensa así:

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Alta Dirección Comité institucional de coordinación de control interno	• Aprobar la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad y evaluar su aplicación. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo. • Evaluar la eficacia de la política frente a la gestión del riesgo institucional. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios, a partir de la información aportada por las instancias de 2ª línea identificadas. • Verificar el cumplimiento de los planes institucionales, estratégicos de la entidad
	Comité de Gestión y Desempeño Institucional	• Asegurar la implementación y articulación de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales. • Generar recomendaciones de mejora a la política de administración del riesgo para su inclusión y aprobación en el Comité Institucional de Coordinación de Control Interno. • Realizar seguimiento y análisis periódico a los riesgos institucionales y proponer mejoras a su estructura.
1ª Línea	Líderes de Procesos Responsable del proyecto	• Promover al interior de su equipo de trabajo el concepto de "administración de riesgo", iniciando por la socialización de la política de riesgo, aprobado por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas,

	Servidores en general	proyectos y planes asociados a su proceso y realizar seguimiento a los controles establecidos en el mapa de riesgo del proceso a cargo. • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso y reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • 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. • Informar a la Oficina Asesora de Planeación o quien haga sus veces (como 2ª línea de defensa) sobre los riesgos materializados en los procesos, programas, proyectos y planes a su cargo. En caso de la materialización de un riesgo no identificado, este debe ser incluido en el mapa de riesgo del proceso correspondiente. • Establecer y aplicar las acciones de mejora requeridas frente al mapa de riesgos correspondiente, una vez se genera el informe de materialización del riesgo. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados • Reportar en la matriz de seguimiento del mapa de riesgos los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Formular el plan de mejoramiento
2ª Línea	Jefatura de Planeación TIC,S y gestión urbanística	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para una adecuada definición de la política de administración del riesgo, el establecimiento de los riesgos al proceso de Direccionamiento acorde con el esquema de procesos actual, o bien el que lo actualice o sustituya cuando existan cambios en dicho esquema de operación. • Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. • Revisar que los controles estes diseñados adecuadamente para la mitigación de los riesgos que se han identificado por parte de la primera línea de defensa y realiza las recomendaciones y seguimiento para el fortalecimiento de estos a través del seguimiento a los controles definidos en el mapa de riesgos. • Informar a la 1ª línea de defensa correspondiente (líder del

		proceso) la materialización de un riesgo no identificado para que sea identificado e incluido en el mapa de riesgo del proceso correspondiente. • Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso) y generar un reporte ejecutivo que permita establecer alertas a la Línea Estratégica sobre retrasos, incumplimientos u otras fallas detectadas Socializar y publicar el mapa de riesgos de cada uno de los procesos. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, valore, evalúe, que 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. • Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad, para su análisis en el CICCI y se adelanten los ajustes que correspondan a este aparte dentro de la presente política. • Proporcionar información sobre la efectividad del Sistema de Control Interno, a través del enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. • Monitoreo la gestión de riesgo y control ejecutada por la primera línea de defensa complementando su trabajo. • Hacer el seguimiento respectivo a todos los riesgos identificados, generando recomendaciones y posibles ajustes a los mapas de riesgos. • Jefe de Planeación (o quien delegue), cuatrimestralmente consolidará el avance sobre la planeación institucional de manera articulada con los temas asociados a los proyectos de inversión, con el propósito de generar alertas en semáforo sobre retrasos o posibles incumplimientos; al tiempo articulará la información sobre eventos (materializaciones de riesgo) asociados a los mismos permitiendo el análisis integral de la gestión del riesgo. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Jefe de la Oficina de Planeación como gestor del proceso de direccionamiento estratégico. • Liderar la gestión de riesgos de seguridad sobre la gestion de TI y de la Información en la entidad. • Asesorar a los líderes de proceso en la identificación de los riegos de seguridad de la información • Supervisar la respuesta a incidentes sobre violaciones de la

		seguridad, informando a la Línea Estratégica sobre sus consecuencias y acciones implementadas. • Generar informes ***semestrales*** sobre fugas de información y los medios externos identificados. • Proponer a la Línea estratégica medidas y mecanismos para mejorar la gestión de seguridad de la información.
2ª Línea	Secretaria General y de Gobierno en articulación con la Jefatura de contratación	• El Jefe de contratación mensualmente, consolida los avances del Plan Anual de Adquisiciones, de acuerdo a cada modalidad de contratación, generando alertas en semáforo frente a retrasos o posibles incumplimientos en los planes, programas o proyectos a los cuales se encuentran asociados los contratos analizados. La fuente para el análisis se basa en los informes de supervisión o interventoría según corresponda de los contratos en ejecución. • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la Secretaria General y de Gobierno como líder del proceso de gestión de recursos.
	Secretaria General y de Gobierno en articulación con el Jefe de Talento Humano	• El Jefe de Talento Humano**,** cuatrimestralmente consolidará el avance sobre PIC, Bienestar, Incentivos y temas de convivencia laboral, mediante un análisis de variables relacionadas con la ejecución de cada uno de estos mecanismos, que permita generar alertas en la ejecución de recursos. En el tema de convivencia generar información sobre quejas reiteradas de acoso laboral, conflictos internos que no ha sido posible resolver y aquellos que llegan a instancia disciplinaria. • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la Secretaria General como líder del proceso de gestión del Talento Humano.
	Secretaria General y de Gobierno	• La Secretaria General y de Gobierno trimestralmente, evalúa la prestación del servicio a los grupos de valor, mediante el análisis de las PQRD y la evaluación de percepción de los usuarios por los diferentes medios de atención, generando alertas en semáforo sobre incumplimiento en términos, reiteraciones de consultas, quejas, denuncias y tutelas que se hayan presentado o que estén en curso. La fuente para el análisis es el sistema de gestion documental- ventanilla unico • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Coordinador de Servicio al Ciudadano como líder del proceso de gestión del Servicio al Ciudadano.

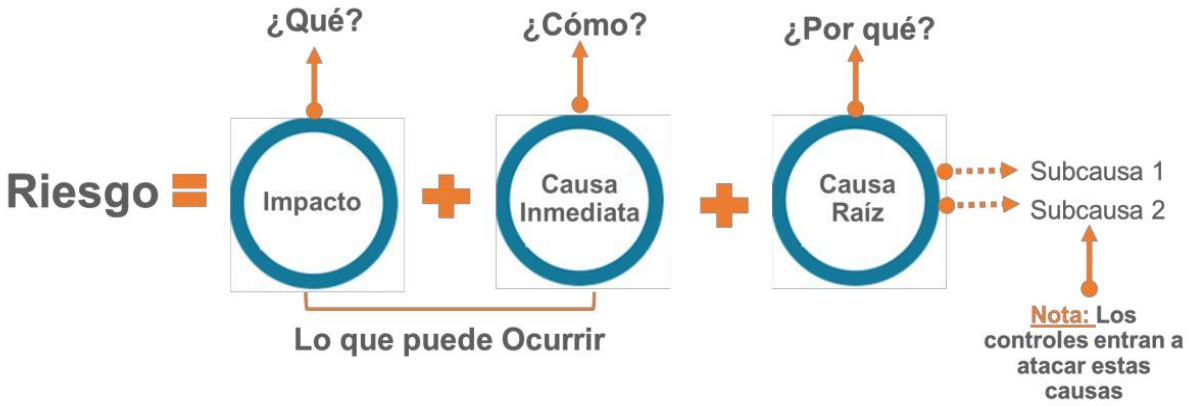
2ª Línea	Equipo jurídico	• El coordinador del equipo Jurídicoo mensualmente, verifica el seguimiento a la gestión judicial adelantada por los abogados asignados, generando información sobre alertas en los procesos que se encuentran abiertos y las cuantías asociadas. La fuente de información es el sistema para la consulta de procesos de la Rama Judicial, el sistema e-Kogui y los informes de los abogados responsables. • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el coordinador del equipo Jurídico como líder del proceso de Defensa Jurídica.
	Jefatura de Planeación TIC y gestión urbanística	• El Jefe de planeación TIC y gestión urbanística mensualmente verifica el avance en los programas y proyectos del área de las TIC generando alertas sobre retrasos o posibles incumplimientos, a fin de tomar las acciones o intervenciones necesarias. • El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Jefe de Planeación TIC y gestión urbanística como líder del proceso de Tecnologías de la Información.
3ª Línea	Jefe de Control Interno o quien haga sus veces	• Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional Coordinador de Control Interno. Para esto tendrá en cuenta los resultados de los seguimientos aplicados por parte de la Jefatura de Planeación TIC y gestión urbanística. • Generar recomendaciones y/o alertas con alcance preventivo a la línea estratégica, a fin de incorporar acciones inmediatas a los temas críticos identificados. • Asesorar y acompañar a la Alta Dirección en la incorporación de estrategias y metodologías para la gestión de riesgo, acorde con las actualizaciones en materia de riesgos corrupción, fiscales, de lavado de activos y otros que se definan en normas nacionales.

11. IDENTIFICACIÓN DE RIESGOS

ESTRUCTURA PARA LA GESTIÓN DEL RIESGO: Identificación, descripción y clasificación de riesgos

DESCRIPCION

Debe de contener todos los detalles necesario tanto para el líder del proceso como para las personas ajenas al proceso identifiquen como se puede manifestar los riesgos, 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, Se debe tener en cuenta la estructura dada por DAFP, esta facilitara su redacción y claridad



Asimismo, es necesario tener en cuenta la clasificación de riesgos definidas por el DAFP- 2022 y que se adoptarán en la en la Alcaldía Municipal San Sebastián de Mariquita:

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

CLASIFICACIÓN DEL RIESGO	DESCRIPCION
Corrupción	Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

	Se establecen sobre el proceso.
Daños Activos Físicos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
Ejecución y Administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fallas Tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
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.
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 , organizacionales	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

Para la Alcaldía municipal de San Sebastián de Mariquita identificamos los siguientes riesgos:

Riesgos de gestión u operativos: En la fase de identificación de riesgos, se describe, se clasifica y se valora el riesgo. Se determina su probabilidad de ocurrencia y el impacto, obteniendo un nivel de riesgo inherente.

Valoración del Riesgo

En la valoración del Riesgo se establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, para establecer la zona de riesgo inicial, es decir, el riesgo inherente; analizando y evaluando los riesgos a través de los controles establecidos, para finalmente establecer la zona de riego final, es decir, la zona residual; se tendrá en cuenta los lineamientos establecidos en la mencionada guía de la función pública.

Determinación de la probabilidad.

La probabilidad se determinará de acuerdo con el número de veces que se pasa por el punto de riesgo en un periodo de un año, según el siguiente criterio:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 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 mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Determinación del impacto.

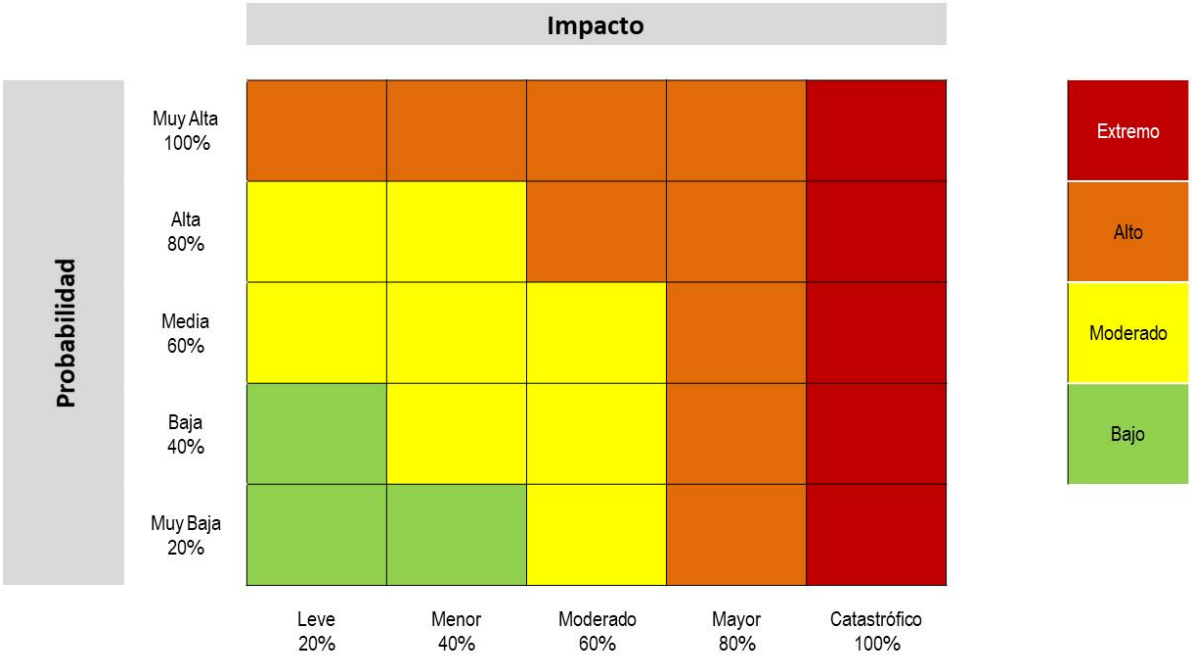
El impacto se determina de acuerdo con la afectación que puede tener el riesgo, el cual puede ser económico, reputacional o por impactos dados por corrupción; aplicando los criterios definidos en la siguiente tabla:

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general 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

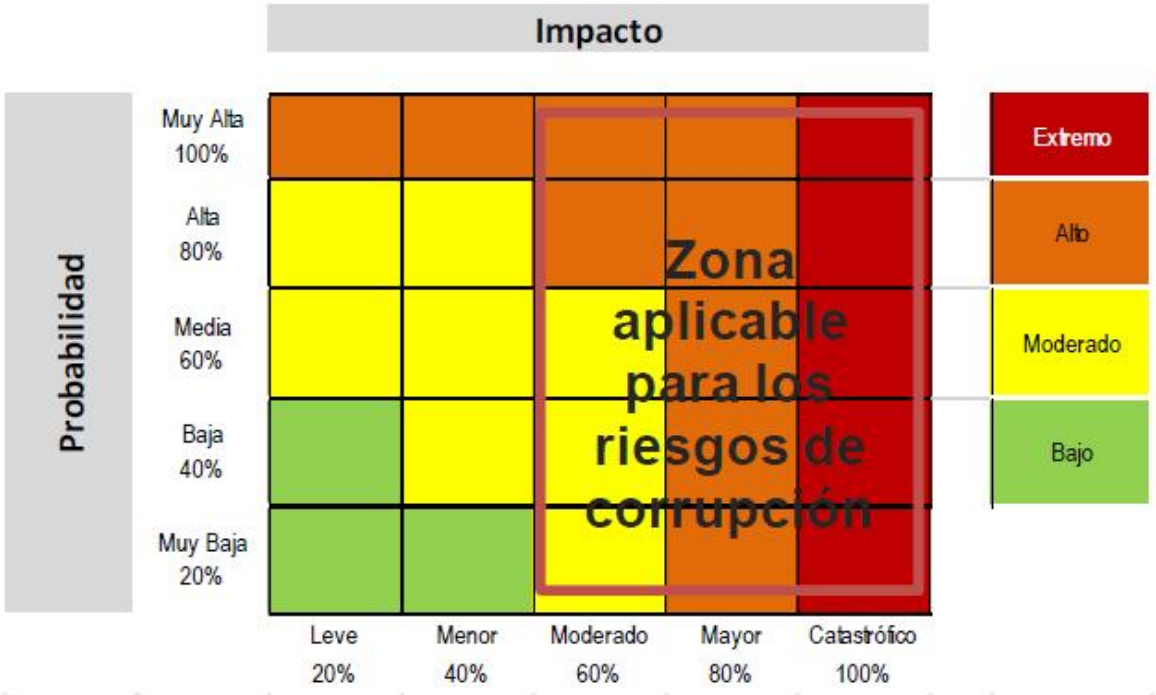
Para los riesgos de corrupción se analizarán únicamente para los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos. Para seleccionar el criterio que le aplica mostrados en la tabla anterior, se aplican los criterios mostrados a continuación:

No.	PREGUNTA: SI EL RIESGO DE CORRPCIÓN 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 misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que 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 los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía 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?		
Responder afirmativamente de UNA a CINCO preguntas(s) genera un **impacto moderado**. Responder afirmativamente de SEIS a ONCE preguntas genera un **impacto mayor.** Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un **impacto catastrófico**.			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Para determinar los niveles de severidad de los riesgos a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor, teniendo en cuenta el siguiente gráfico:



Analizado la probabilidad y el Impacto para los Riesgos de Corrupción aplicando controles, se obtiene matriz de calor para riesgos de corrupción de acuerdo con el siguiente cuadro:



Identificación del control y valoración del riesgo residual

Los controles una vez se identifiquen deben ser coherentes y estar dirigidos a minimizar las causas inmediatas y su redacción se realiza de acuerdo con lo establecido en el numeral 3..2.2.1 de la guía de administración del riesgo y diseño de controles para entidades públicas.

Para el análisis y valoración de los controles, teniendo en cuenta las características relacionadas con la eficiencia y la formalización, se tiene en cuenta la siguiente tabla:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de	15%

Características			Descripción	Peso
			manera automática sin la intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	25%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se 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: Esta evaluación es realizada en el formato de Mapa de Riesgo de la entidad.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, es decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control, y de esta forma se calcula el riesgo residual.

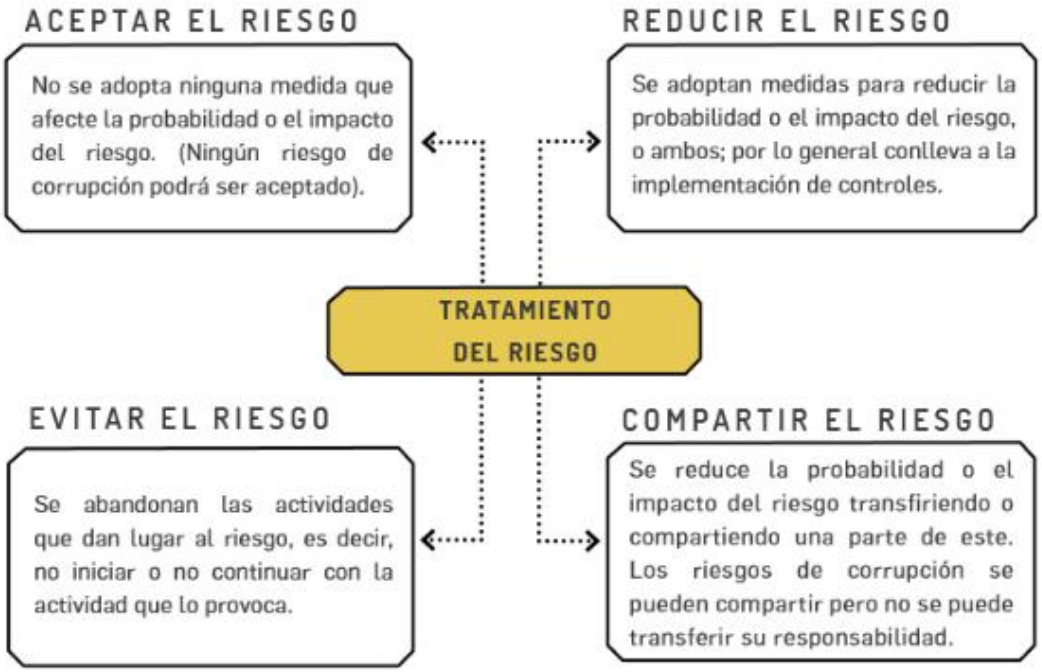
Los controles preventivos y detectivos reducen en el riesgo residual la probabilidad; y los correctivos el impacto.

Para los controles que no están implementados, se establece un plan de tratamiento de riesgos. Para los riesgos de seguridad de la información, la Oficina de Planeación, TIC y gestión urbanística coordinará con los responsables la implementación de los controles definidos y el respectivo plan de tratamiento de riesgos.

Estrategias para combatir el riesgo

Se analiza frente al riesgo residual, esto para procesos en operación, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente, en el siguiente cuadro se identifican las opciones para combatir el riesgo teniendo en cuenta el Plan de Acción a que allá lugar.

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control



Clasificación actividades de control

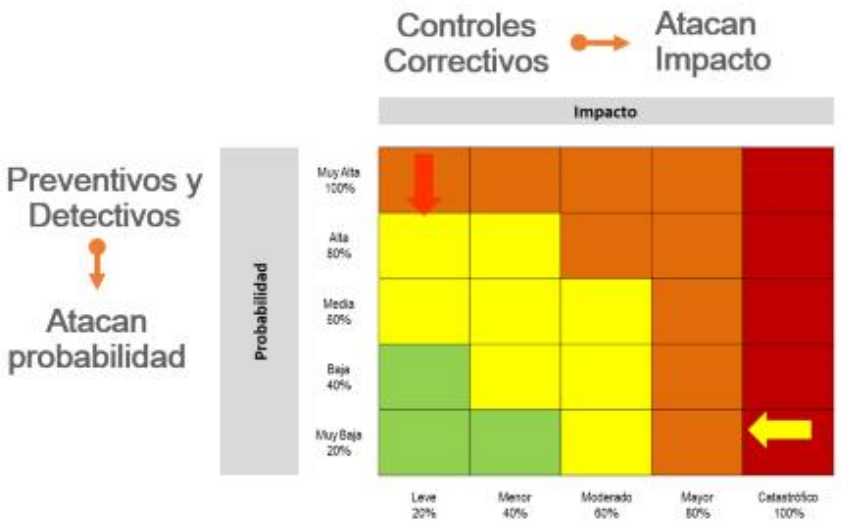
- ✓ **Controles preventivos** Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.

- ✓ **Controles Detectivos** Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal , pero generan reprocesos.

- ✓ **Control Correctivo:** Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal . Estos controles tienen costos implícitos.

Los controles se ejecutan de manera manual y de acuerdo al resultado de los controles aplicados se obtiene el riesgo residual , se identifica a través del mapa de calor

Movimiento en la matriz de calor acorde con el tipo de control



ESTRATEGIAS PARA COMBATIR RIESGOS

se define el "**Plan de Acción"**, en el que se determinan las acciones a desarrollar para los riesgos, de acuerdo con su tipología y los niveles de aceptación.

Acciones a realizar

ACEPTAR Se determina para los riesgos cuyo resultado, una vez aplicados los controles, se encuentra en el nivel de RIESGO RESIDUAL LEVE, MENOR o MODERADO. Estos riesgos requieren monitoreo y seguimiento periódico por parte de los líderes de procesos.

En esta opción se considera la opción TRANSFERIR, cuando se considera que la mejor estrategia es tercerizar o trasladar el riesgo a través de pólizas.

EVITAR Decisión que se adopta cuando después de un análisis se considera que el riesgo es demasiado alto y lo mejor es NO asumir la actividad que genera el riesgo y por tanto plantear una diferente.

REDUCIR. Se determina para los riesgos cuyo resultado, una vez aplicados los controles, se encuentran en el nivel ALTO o CASTASTROFICO. Estos riesgos requieren monitoreo y seguimiento permanente por parte de los líderes de procesos y, además, exigen la formulación de plan de acción.

Para los riesgos de corrupción, , no hay aceptación. En consecuencia, este tipo de riesgos no podrán valorarse en un nivel residual leve o menor, por tanto, siempre requerirán la definición de acciones para reducir el nivel del riesgo.

El plan de acción se deberá de formular y debe contener como mínimo la siguiente información :

Riesgo, control , actividades ejecutadas , responsable, fecha de inicio, fecha fin, indicador de cumplimiento de la acción , fecha de seguimiento y la observación de control interno.

12. RIESGOS FISCALES

Control fiscal interno y prevención del riesgo fiscal: - propósito Prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representado al menoscabo, disminución y perjuicio , detrimento, perdida o deterioro de los bienes o recursos públicos, o a los interés patrimoniales del Estado (Decreto 403, 2020, art 6) .

Definición

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la guía de la Función Pública, la cual es armónica con la norma ISO 31000, define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

fuente DAFP 2022

Identificación de los Riesgos Fiscales

Establecer los puntos de riesgo fiscal y las circunstancias inmediatas.

Puntos de Riesgo Fiscal son situaciones en las que potencialmente se genera riesgo fisca, es decir, son aquellas actividades de administración , gestión, ordenación , ejecución, manejo adquisición , planeación, conservación , custodia, explotación, enajenación , consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, asi como a la recaudación, manejo e inversión de sus rentas . (Articulo 3 Ley 610 de 2000)

Circunstancia inmediata es aquella situación o actividad bajo la cual se representa el riesgo, pero no constituye la causa – causa raíz- para que se represente el riesgo.

Identificación de áreas de impacto Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Identificacion de la causa raiz o potencial hecho generador

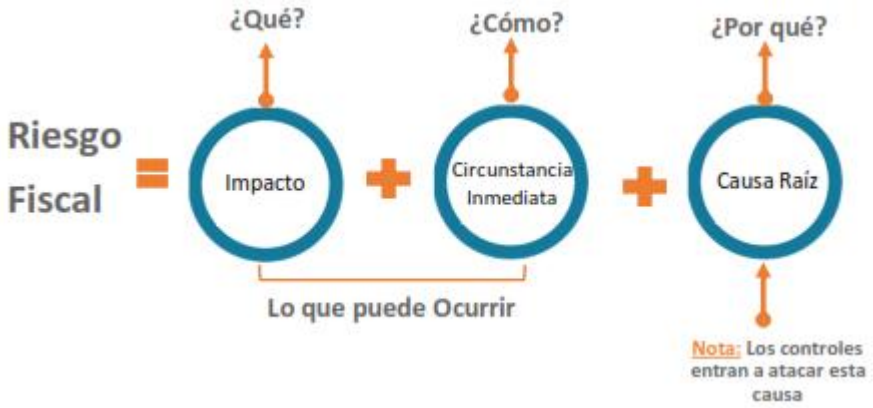
La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

Descripción del Riesgo Fiscal

A continuación se presenta la estructura definida en la Guía de Administración de Riesgo - 2022

- ✓ Iniciar con la oración – *posibilidad de,* debido a que nos estamos refiriendo al evento potencial.
- ✓ Impacto : corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- ✓ Circunstancia inmediata : corresponde al como . se refiere aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica – causa raíz – para que se presente el riesgo.
- ✓ Causa Raíz : Corresponde al porque; que es el evento acción u omisión) que de presentarse es causante , es decir , generado directo, causa eficiente, o adecuada. Es la condición necesaria , de tal forma que , si ese hecho no se produce, el daño no se genera.

Estructura en imagen



FUE

NTE DAFP 2022

Valoración de los Riesgos fiscales

Evaluación de los riesgos

Se establece la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impactos inherentes.

Probabilidad

Es la posibilidad de ocurrencia del riesgo fiscal, se determina el numero de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año – numero de veces que se realizan las actividades que represente la gestión fiscal.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 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 mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Impacto

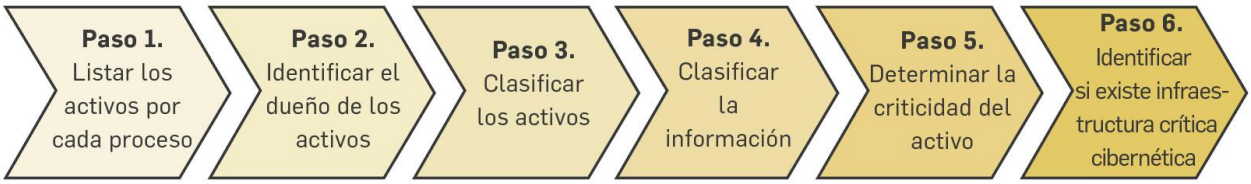
Considerando la naturaleza y alcance del riesgo fiscal, éste ***siempre tendrá un impacto económico***, toda vez que el efecto dañoso **siempre** ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública, para ello se aplicara la tabal definida en la Guía de Administración de Riesgo.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general 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

13. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para la identificación de los riesgos de Seguridad de la Información, se debe tener en cuenta la Política de Seguridad y Privacidad de la Información que propende por preservar las características de confidencialidad, integridad y disponibilidad de los activos de información que hacen parte de cada uno de los procesos institucionales, para lo cual es fundamental identificar y valorar los activos de información institucionales. Estos activos se identifican teniendo en cuenta los siguientes pasos:

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



Para la valoración de riesgos inherentes de la seguridad de los diferentes activos de información identificados se requiere que sus propietarios identifiquen, dentro del contexto interno y externo de la entidad, las consecuencias que tendría la pérdida de su confidencialidad, integridad o disponibilidad, en el peor caso posible, es decir sin tener en cuenta medidas de seguridad existentes en la entidad, por lo tanto, se debe tener en cuenta la perdida de:

- Confidencialidad
- Integridad
- Disponibilidad

Los activos de información se clasifican en:

- Físico
- Información
- Personal
- Procesos
- Red
- Servicios
- Software

La valoración de los activos de información se realiza en una escala de 1 a 5, teniendo en cuenta los siguientes criterios:

Valoración CID	Descripción
1	Daño insignificante
2	Daño menor
3	Daño considerable
4	Daño grave
5	El cumplimiento de la misionalidad institucional se ve amenazada por la pérdida de la confidencialidad, integridad o disponibilidad del activo de información

Para la valoración de los activos de información se tiene en cuenta la siguiente tabla:

Una vez identificados y valorados los activos de información de cada uno de los procesos, se analizan las amenazas que pueden explotar vulnerabilidades existentes en estos, evaluándolas de 0 a 3, de acuerdo con la siguiente tabla:

Nivel de Amenaza	Descripción	Justificación
0	La amenaza no está presente en el entorno del activo dentro del contexto de la organización.	Requiere
1	La amenaza se considera presente en el entorno del activo dentro del contexto de la entidad y con baja probabilidad de que explote vulnerabilidades dentro del alcance.	Requiere
2	La amenaza se considera presente en el entorno del activo dentro del contexto de la entidad y con media probabilidad de que explote vulnerabilidades dentro del alcance.	No requiere
3	La amenaza se considera presente en el entorno del activo dentro del contexto de la entidad y con alta probabilidad de que explote vulnerabilidades dentro del	No requiere

	alcance.	

Del mismo modo se realiza la evaluación de vulnerabilidades de los diferentes activos de información, para lo cual se tiene en cuenta la siguiente tabla:

Vulnerabilidad	Descripción	Justificación
0	La vulnerabilidad no aplica al activo dentro del contexto de la entidad, por lo que el control no se aplica.	Requiere
1	Es muy improbable que la vulnerabilidad sea explotada, ya que el control está implantado de forma eficiente y ha sido auditado sin registrarse incumplimientos.	Requiere
2	Es poco probable que la vulnerabilidad sea explotada en el futuro, ya que el control está implantado de forma eficiente.	Requiere
3	Es probable que la vulnerabilidad sea explotada en el futuro, ya que el control se ha implantado parcialmente o de forma deficiente.	Requiere
4	Es muy probable que la vulnerabilidad sea explotada en el futuro ya que el control no se ha implantado.	No requiere
5	La vulnerabilidad ha sido explotada en el pasado, más allá del nivel de implantación del control.	No requiere

A partir de la valoración de confidencialidad, disponibilidad e integridad de los diferentes activos de información y el análisis de amenazas y vulnerabilidades, se obtiene el nivel de riesgos, así:

$$R_a = I_a * Max(A_a * V)$$

R_a: Riesgo sobre el activo.
I_a: Impacto sobre el activo en términos de confidencialidad, integridad y disponibilidad.
A_a: Amenaza en el entorno sobre el activo.
V: Vulnerabilidad.

A continuación, se presenta el mapa de calor de gestión de riesgos de seguridad de la información:

	Nivel de Amenaza	1					2					3				
	Nivel de Vulnerabilidad	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Valor del Activo	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30

	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75
		Nivel de Riesgo														

Los datos reflejados en la tabla anterior se interpretarán de la siguiente manera:

Nivel de Riesgo	Descripción
1 – 24 Bajo	No es necesario adoptar ninguna medida. El nivel de riesgo es suficientemente bajo y no justifica la implantación de controles adicionales.
25 – 48 Moderado	La dirección de la empresa, o un delegado de esta, determinará el nivel de los riesgos que son aceptables o no a su juicio. El Responsable de Seguridad que gestiona el SGSI determinará los controles que tendrán que aplicarse para mitigar los riesgos.
49 – 75 Alto	El nivel de riesgos no es aceptable, y sólo se podrán excluir controles que los mitiguen justificando dicha exclusión por parte de la dirección de la empresa. El Responsable de Seguridad que gestiona el SGSI determinará los controles que tendrán que aplicarse para mitigar los riesgos.

La gestión del riesgo se realiza a través de tres estrategias, las cuales son:

- Evitar .
- Reducir .
- Mitigar

Aceptar el riesgo

La Entidad puede aceptar riesgos que no tratará de ninguna manera en los casos que:

- El riesgo sea menor o igual al nivel de riesgo aceptable.
- El coste de tratar el riesgo sea mayor que el daño que pueda causar su impacto.
- El coste de tratar el riesgo no pueda ser asumido económicamente. En este caso deberán considerarse opciones adecuadas al presupuesto para el tratamiento, aunque no sean las idóneas.

Para cualquiera de estas situaciones, se justificará debidamente las razones por las que el riesgo se acepta.

Tratar el riesgo

La Entidad decidirá, la prioridad en la implantación de las medidas de tratamiento de riesgo, en proporción al nivel de riesgo, la facilidad de la implantación, el coste o a los cambios en la entidad.

1. **Riesgo ALTO**: Si el nivel de riesgo resultante para un activo es igual o superior a 49, se seleccionarán los objetivos de control y controles que mitiguen el riesgo a un nivel aceptable y que encajen con los requisitos establecidos por la Entidad. En relación con los activos y a sus vulnerabilidades/amenazas asociadas, se implantarán todos los controles adicionales que tengan un efecto positivo en la misionalidad institucional y en los procesos existentes y cuyo coste sea aceptable.

2. **Riesgo MODERADO**: Se puede aceptar un riesgo con un nivel entre 25 y 49 por cualquiera de las razones expuestas a continuación:

    a) El control o el proceso asociado no está alineado con la cultura de la organización.
    b) El personal necesario para su operación no está disponible.
    c) Los recursos económicos necesarios no están disponibles.
    d) No existe un beneficio claro para la Entidad.
    e) El coste de implantación del control supera el coste del activo que protege o el coste de una brecha de seguridad actual o futura.

La aceptación del riesgo debe quedar documentada. En caso de no aceptación del riesgo, se actuará, como se indica para el caso de riesgo ALTO, seleccionando los procedimientos, mejores prácticas y mecanismos que mitiguen el riesgo a un nivel aceptable.

3. **Riesgo BAJO**: Los niveles de riesgo entre 1 y 24 son bajos y no requieren actuación ninguna.

Se determina que un riesgo ALTO es inaceptable para la Entidad, a menos que así lo decida la línea de defensa estratégica y sobre el que dependa la propiedad y el derecho de uso del activo afectado mediante la justificación de dicha decisión.

Transferir el riesgo

Cuando sea conveniente, la entidad podrá transferir el riesgo a otras entidades. En caso de optar por transferir un riesgo, las acciones tomadas deben quedar documentadas y ser revisadas. Las responsabilidades transferidas se reflejarán en acuerdos de nivel de servicio.

Se registrarán las actuaciones llevadas adelante en la transferencia de los riesgos.

Evitar el riesgo

La Entidad también puede optar por evitar el riesgo cesando un proceso o actividad o modificando la forma en que este se lleva a cabo. En caso de optar por evitar un riesgo, las acciones tomadas deben quedar documentadas y ser revisadas.

Si el proceso o actividad son modificados, deberá realizarse el análisis de riesgos para el proceso o actividad modificada, no así en caso de cese de este.

Se registrarán las actuaciones llevadas adelante para evitar los riesgos.

Aceptación del riesgo residual

El riesgo residual para cualquiera de los activos y una vez aplicados las medidas de control previstas deberían situarse en un rango de valores por debajo del valor de riesgo aceptable determinado por la Entidad.

Para aquellos casos en que, tras el tratamiento con los controles previstos, se determine un nivel de riesgo moderado, se deberá obtener la aprobación de la línea de defensa estratégica para aceptar el riesgo residual resultante, lo cual deberá ser documentado.

Vulnerabilidad Residual	Descripción
0	La vulnerabilidad residual no aplica al activo porque la amenaza no aplica, o porque el conjunto de controles no aplica.
1	Es muy improbable que la vulnerabilidad residual sea explotada, ya que el conjunto de controles estará implantado y auditado.
2	Es poco probable que la vulnerabilidad residual sea explotada en el futuro, ya que el conjunto de controles estará implantado.
3	La vulnerabilidad residual es parcial ya que el activo ha sido evaluado metodológicamente y se ha decidido aceptar su riesgo.

Realizada la gestión de riesgos, se obtiene la Declaratoria de Aplicabilidad y el Plan de Tratamiento de Riesgos.

De conformidad con la Política de Seguridad y Privacidad de la Información, lo anterior se realiza a través del aplicativo establecido por la Oficina de Planeación, TIC y Gestión Urbanística, quien coordina todo el proceso de identificación de los activos de información con los responsables de los procesos y establece las valoraciones con los mismos. Así mismo establece los planes de gestión de riesgos a los cuales tenga lugar y realiza los seguimientos a los mismos.

14. OTRAS DISPOSICIONES CON RELACIÓN A LA GESTIÓN DE LOS RIESGOS

- Para cada riesgo de seguridad de la información, se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. La entidad acoge las tablas establecidas en el Anexo 4 del Modelo Nacional de Gestión de Riesgos de Seguridad de la información para entidades públicas.

- Los responsables de los procesos deben verificar que los riesgos se encuentren actualizados, se apliquen los controles definidos con sus acciones, para un adecuado monitoreo de los mismos, de lo cual se dejará constancia en el Formato MAPA DE RIESGOS.
- La Política de Administración del Riesgo se revisará cada vez que sea requerido por parte del Representante de la Alta Dirección teniendo en cuenta los comentarios y lineamientos del Comité Institucional de Coordinación de Control Interno.
- Los responsables de los procesos deben identificar las situaciones que puedan afectar el desarrollo de las actividades de los procesos o el logro de los objetivos propuestos y establecer los controles necesarios y su pertinencia para evitar que los riesgos se materialicen, los cuales deben ser formalizados y comunicados al Proceso Administración del Sistema Integrado de Gestión, a efectos de mantener actualizados los mapas de riesgos.
- Los responsables de los procesos misionales deben identificar los riesgos que puedan afectar cada uno de los instrumentos de política formulados y determinar los controles que permitan disminuir su impacto y/o la probabilidad de ocurrencia.
- Los responsables de los procesos deben garantizar los recursos (físicos, financieros y de talento humano) que sean requeridos para mantener los controles que se establezcan, para evitar que se materialicen los riesgos.
- Los responsables de los procesos deben mantener las evidencias de la aplicación de los controles definidos para los riesgos identificados.

15. SEGUIMIENTO AL CUMPLIMIENTO DE LA POLÍTICA, MONITOREO Y REVISIÓN DE LOS RIESGOS

La aplicación de la Política de Administración del Riesgo es responsabilidad de todos los servidores y contratistas de la entidad, la cual puede ser revisada por parte de la Línea Estratégica en cualquier momento, de acuerdo con las directrices que establezca el Comité Institucional de Coordinación de Control Interno. Las acciones que de esta revisión surjan deben ser adoptadas e implementadas por los responsables, de acuerdo con su nivel de responsabilidad.

16. SEGUIMIENTO Y EVALUACIÓN DEL MAPA DE RIESGO

Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos, dejando como constancia la matriz de seguimiento adoptada debidamente diligenciada.

Los líderes de proceso monitorean constantemente los controles definidos para los riesgos y las acciones del plan de acción, cuando haya lugar, remitiendo a la oficina de control interno el respectivo monitorie con evidencias.

La Oficina de Planeación, Tic y Gestión Urbanística, cumplirá con las acciones de monitoreo de acuerdo con las responsabilidades como segunda línea de defensa, de manera cuatrimestral.

Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos y la efectividad de los controles incorporados en el mapa de riesgos institucional.

La Oficina de Control Interno lleva a cabo el seguimiento a la administración del riesgo, de conformidad con lo indicado en los documentos “Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces” y como se determina en el título precedente de Roles y Responsabilidades.

La Oficina de Control Interno presentará un informe semestral sobre los resultados de la evaluación de la efectividad del sistema de Control Interno - SCI, acorde con la evaluación de los controles definidos en los mapas de riesgos y de los riesgos de procesos, en el cual se consigne, cuando sea el caso, la materialización, la creación, la modificación o la eliminación de alguno de los riesgos.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.
- Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo

17. COMUNICACIÓN Y SOCIALIZACIÓN DE LA POLÍTICA DE GESTIÓN DEL RIESGO

La política de administración del riesgo será comunicada a todos los niveles de la organización, mediante alguno de los siguientes canales:

- Página WEB de la Entidad
- Correos electrónicos
- Procesos de Formación y Capacitación
- Ejercicios de Inducción y Re-Inducción

A través de estos canales se comunica o socializa contenidos relacionados con la gestión de los riesgos y aquellos orientados a generar conocimiento en los funcionarios y contratistas de la entidad.

CONTROL DE VERSIONES			
VERSIÓN	**MOTIVO DEL CAMBIO**	**RESPONSABLE**	**FECHA**
1.0	Adopcion de documento	Jefe oficina de Planeacion, Tic y Gestion Urbanistica	2023
2.0	Articulación y actualización con los lineamientos de la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 06 en cuanto a los lineamientos de niveles de Responsabilidad y autoridad frente a la Administración del riesgo en la entidad (acorde con el esquema de líneas de defensa). análisis de riesgo fiscal y de corrupción.	Jefe oficina de Planeacion, Tic y Gestion Urbanistica	2024

APROBACION		
	NOMBRE	**FIRMA VISTO BUENO**
ELABORÓ	**CARLOS ALBERTO LÓPEZ RODRÍGUEZ**	
	Contratista de Apoyo a la Gestión	
REVISÓ	**HARRINSON ACOSTA OLAYA**	
	Jefe de Planeación, TIC y Gestión Urbanística	
APROBÓ	**COMITÉ INSTITUCIONAL DE CONTROL INTERNO**	
	Acta No.003 del 20 de noviembre de 2024	