TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1. OBJETIVO

Generar el conocimiento para la Administración de los Riesgos de gestión, corrupción y seguridad de la información y los niveles de responsabilidad, con el propósito de mitigar o eliminar situaciones o eventos que afectan el logro de los objetivos institucionales, así como la identificación de oportunidades para el mejoramiento continuo de los procesos y sus servidores, fortaleciendo la cultura de control al interior de la Administración Municipal.

2. ALCANCE

La Política de Administración del Riesgo hace parte de la gestión institucional, es estratégica, basada en el modelo de operación por procesos y en los riesgos de corrupción, y se aplica a todos los procesos de la Alcaldía Municipal.

El desarrollo de la política de administración del riesgo implica establecer el contexto estratégico que es la base para la identificación de riesgos y oportunidades para cada proceso, los factores internos y externos del riesgo, determinar las posibles causas internas y externas, establecer los efectos, definir el riesgo y consolidar la información en una matriz que permita visualizar la relación de dichos riesgos en cada uno de los procesos institucionales.

3. TERMINOS Y CONCEPTOS

3.1 TÉRMINOS

- **Activo**: en el contexto de seguridad de la información 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.
- **Amenazas**: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **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.
- **Confidencialidad**: propiedad de la información que la hace no disponible, o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento, o un beneficio.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **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:** Son las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad**: propiedad de exactitud y completitud.
- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, que transforma elementos de entrada en elementos de salida para generar un valor.
- **Plan Anticorrupción y de Atención al Ciudadano** - **PAAC**: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **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.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: 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 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.
- **Riesgo Inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite 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.
- **Severidad:** Es la magnitud de las posibles consecuencias adversas del riesgo.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
- **Control interno contable:** Es el proceso que bajo la responsabilidad del representante legal o máximo directivo de la entidad, así como de los responsables de las áreas financieras y contables, se adelanta en las entidades, con el fin de lograr la existencia y efectividad de los procedimientos de control y verificación de las actividades propias del proceso contable, de modo que garanticen razonablemente que la información financiera cumpla con las características fundamentales de relevancia y representación fiel de que trata el Régimen de Contabilidad Pública.

Conocimiento de la Entidad – Antes de aplicar la metodología: Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos, planeación institucional, entre otros aspectos, permitiendo conocer y entender la entidad, y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general:

- **Modelo de Operación por Procesos:** El modelo de operación por procesos es el estándar organizacional que soporta la operación de la entidad pública, integrando las competencias constitucionales y legales que la rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos institucionales. Pretende determinar la mejor y más eficiente forma de ejecutar las operaciones de la entidad.
- **Planeación Estratégica:** Ejercicio emprendido por el equipo directivo de una entidad, en el que, a partir del propósito fundamental de la misma, las necesidades de sus grupos de valor, las prioridades de los planes de desarrollo (nacionales y territoriales) y su marco normativo, define los grandes desafíos y metas institucionales a lograr en el corto, mediano y largo plazo, así como las rutas de trabajo a emprender para hacer viable la consecución de dichos desafíos.
- **Cadena de Valor:** Describe una relación secuencial y lógica entre insumos, actividades, productos y resultados, en la que se añade valor a lo largo del proceso de transformación total.
- **Mapa o Red de Procesos:** Es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación y sus interacciones.
- **Caracterización de Procesos:** Estructura que permite identificar los rasgos distintivos de los procesos. Establece su objetivo, la relación con los demás procesos, los insumos, su transformación a través de las actividades que desarrolla y las salidas del proceso, se identifican los proveedores y clientes o usuarios, que pueden ser internos o externos.
- **Misión:** Constituye la razón de ser de la entidad; sintetiza los principales propósitos estratégicos y los valores esenciales que deben ser conocidos, comprendidos y compartidos por todas las personas que hacen parte de la entidad.
- **Visión:** Es la proyección de la entidad a largo plazo que permite establecer su direccionamiento, el rumbo, las metas y lograr su desarrollo. Debe ser construida y desarrollada por la Alta Dirección de manera participativa, en forma clara, amplia, positiva, coherente, convincente, comunicada y compartida por todos los miembros de la organización.
- **Objetivos Estratégicos:** Es la expresión de los logros que se espera que las entidades públicas alcancen en el largo y mediano plazo, en el marco del cumplimiento de su propósito fundamental y de las prioridades del gobierno.
- **Objetivo del Proceso:** Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción por lo tanto debe iniciarse con un verbo fuerte como: Establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: Medibles, realistas y se deben evitar frases subjetivas en su construcción.

3.2 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:

- **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 poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto**.**

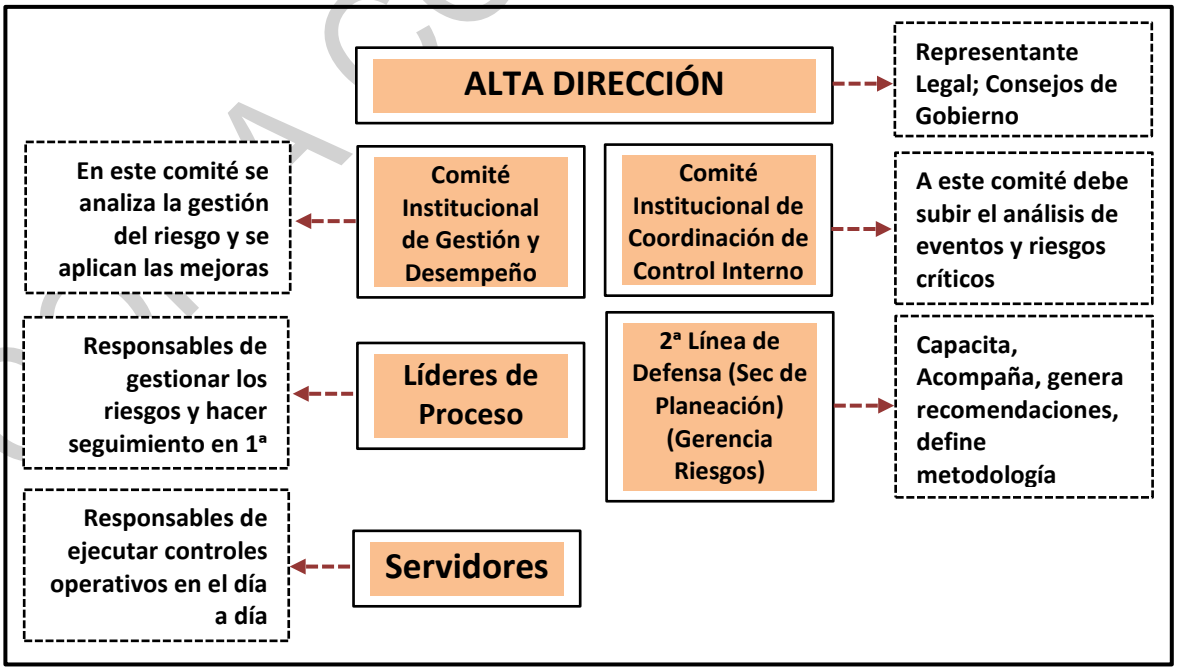
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.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

4. ESTRUCUTURA PARA LA GESTION DEL RIESGO

4.1 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, Decreto 0035 de marzo de 2019 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Figura 1. Operatividad Institucional para la Administración del Riesgo



5. DOCUMENTOS DE REFERENCIA

- Mapa de Riesgos de Gestión
- Plan Anticorrupción y Atención al Ciudadano - PAAC
- Mapa de Riesgos de Corrupción

6. NORMATIVIDAD

- Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado; en el literal f del Artículo 2 establece como uno de los objetivos del Sistema de Control interno: definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

- Ley 489 de 1998. Estatuto básico de organización y funcionamiento de la Administración Pública.

- Decreto 4485 de 2009, Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos Generales literal g) "establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad" cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

- Ley 1474 de 2011, Estatuto Anticorrupción. Artículo 73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.

- Decreto 2641 de 2012. Por el cual se reglamentan los artículos **73** y **76** de la Ley 1474 de 2011. Señala como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento *"Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano"*.

- Norma Técnica Colombiana NTC ISO 9001. Especifica los requisitos para la implementación de un Sistema de Gestión de la Calidad dirigido a garantizar la satisfacción del cliente, en el numeral 6.1 define que las Organizaciones deben establecer las acciones para abordar los riesgos y oportunidades, proporcionales al impacto potencial en la conformidad con los productos y servicios.

- Decreto 1083 de 2015, por el cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Título 23 Art. 2.2.23.1 - Adopta la actualización de la Norma Técnica de

Calidad en la Gestión Pública NTCGP 1000 Versión 2009, la cual establece las generalidades y los requisitos mínimos para establecer, documentar, implementar y mantener un Sistema de Gestión de la Calidad en los organismos, entidades y agentes obligados conforme al artículo 2° de la Ley 872 de 2003. La Norma Técnica de Calidad en la Gestión Pública, NTCGP 1000 versión 2009 es de obligatoria aplicación y cumplimiento. Art. 2.2.23.2. El establecimiento y desarrollo del Sistema de Gestión de la Calidad en los organismos y entidades públicas a que hace referencia el artículo 2° de la Ley 872 de 2004, será responsabilidad de la máxima autoridad de la entidad u organismo correspondiente y de los jefes de cada dependencia de las entidades y organismos, así como de los demás empleados de la respectiva entidad.

- Decreto 124 del 26 de enero de 2016 “Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al “Plan Anticorrupción y de Atención al Ciudadano”, se estableció en su Artículo 2.1.4.1 como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011.

- Resolución 193 del 5 de mayo de 2016 de la Contaduría General de la Nación, incorpora, en los Procedimientos Transversales del Régimen de Contabilidad Pública, el Procedimiento para la evaluación del control interno contable.

- Decreto 648 de 2017 “Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública”.

- 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”.

- Resolución-0489 del 29 de diciembre de 2017.

- Norma Internacional ISO 31000:2018 “Administración/Gestión de riesgos — Lineamientos guía”

- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 – diciembre de 2020

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad digital. Versión 4 de 2018.

- Política de Operación Riesgos de la Función Pública, 2018

- Anexo 4 de la Guía DAFP 2018 - Lineamientos para la gestión de riesgos de seguridad de la información en Entidades Públicas.

- Guía para la Gestión del Riesgo de Corrupción de la Secretaría Administrativa de la Presidencia de la República.

7. DESARROLLO Y/O DESCRIPCIÓN

7.1 PRESENTACIÓN

Para la Alcaldía de Bucaramanga es de gran importancia el cumplimiento de sus objetivos misionales a través del diseño e implementación de acciones soportadas en la prevención de los riesgos, a través de controles que promuevan la generación de comportamientos éticos y conlleven a la construcción de una cultura de buen gobierno, que impida la materialización de riesgos de gestión, corrupción y seguridad de la información.

Es así como la Administración Municipal, con base en la normatividad vigente y la metodología establecida por el Departamento Administrativo de la Función Pública a través de la Guía para la administración del riesgo y el diseño de controles en entidades públicas 2020, diseña la Política de Administración del Riesgo como mecanismo para fortalecer el control en los procesos administrativos y misionales, en concordancia con las directrices en materia de gestión pública, los parámetros del Modelo Estándar de Control Interno-MECI en lo referente a las líneas de defensa, y el enfoque del Modelo Integrado de Planeación y Gestión- MIPG.

La Política de Administración del Riesgo es la declaración del compromiso del equipo directivo de la Alcaldía de Bucaramanga, a través de la cual se establecen lineamientos para la identificación, análisis, seguimiento, monitoreo y evaluación de los riesgos, que puedan afectar los resultados de la gestión y permitir el cumplimiento de las metas establecidas en el Plan de Desarrollo Municipal.

Este documento involucra, mediante un ámbito estratégico y líneas de defensa, a todos los servidores de la Entidad, soportándose en los mecanismos de comunicación disponibles, y cubriendo todas las responsabilidades institucionales y las propias de cada servidor, definidas en la normativa aplicable y la documentación de cada proceso.

La Política de Administración del Riesgo es reconocida como una parte integral de las buenas prácticas gerenciales, que posibilitan una mejora continua en la toma de decisiones. Las temáticas relacionadas con la gestión de riesgos, son definidas mediante directrices para la identificación de riesgos de gestión y de corrupción, entre otros; las causas generadoras; las consecuencias o efectos de la materialización; la matriz de calor y las zonas de riesgo; las escalas para la calificación de la probabilidad e impacto; las actividades de control y su análisis; la valoración después de controles; las opciones y acciones de tratamiento según la valoración residual; el establecimiento de planes de contingencia; así como los ciclos de monitoreo y evaluación, y el respectivo seguimiento.

La Alcaldía de Bucaramanga define su Política de Administración de Riesgos tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión en los procesos que integra los sistemas de gestión de la calidad y de desarrollo administrativo, así como los del Modelo Estándar de Control Interno, en lo referente a las líneas de defensa; los lineamientos de la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas,*" del Departamento Administrativo de la Función Pública versión 5 de 2020 que articula los riesgos de gestión, corrupción y de seguridad de la información, y el Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018.

7.2 OBJETIVOS ESPECIFICOS

a) Orientar y fortalecer la toma de decisiones oportuna a través de la identificación, análisis, valoración y tratamiento de los riesgos al interior de la Administración Municipal, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos establecidos con los ciudadanos, servidores e instituciones públicas.

b) Proteger los recursos de la institución, resguardándolos contra la materialización de los riesgos.

c) Introducir dentro de los procesos y procedimientos las acciones de control, como resultado de la administración del riesgo.

d) Comprometer a los servidores públicos en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos, que faciliten el desarrollo institucional, manteniendo la buena imagen y las buenas prácticas.

e) Identificar las oportunidades dentro del contexto interno y externo a la Alcaldía de Bucaramanga, que permitan la mejora continua en la gestión.

f) Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores de la entidad (esquema de las líneas de defensa) en los riesgos de gestión.

g) Gestionar los riesgos del proceso contable a fin de promover la consecución de las características fundamentales de relevancia y representación fiel de la información como producto del proceso contable, definiendo e implementando los controles que sean necesarios para que se lleven a cabo las diferentes actividades del proceso contable de forma adecuada.

h) Establecer acciones de monitoreo continuo y control que permitan garantizar que las respuestas a los riesgos institucionales se lleven de manera adecuada y oportuna.

8. RESPONSABILIDAD Y ROLES

Tabla 1. Responsabilidad y Roles

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Estratégica	Alta Dirección - Alcalde Municipal, Comité Institucional de Coordinación de Control Interno	• Establecer y aprobar la Política de Administración del Riesgo y su actualización. • 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. • Evaluar el estado del sistema de control interno y aprobar las modificaciones actualizaciones y acciones de fortalecimiento de este.

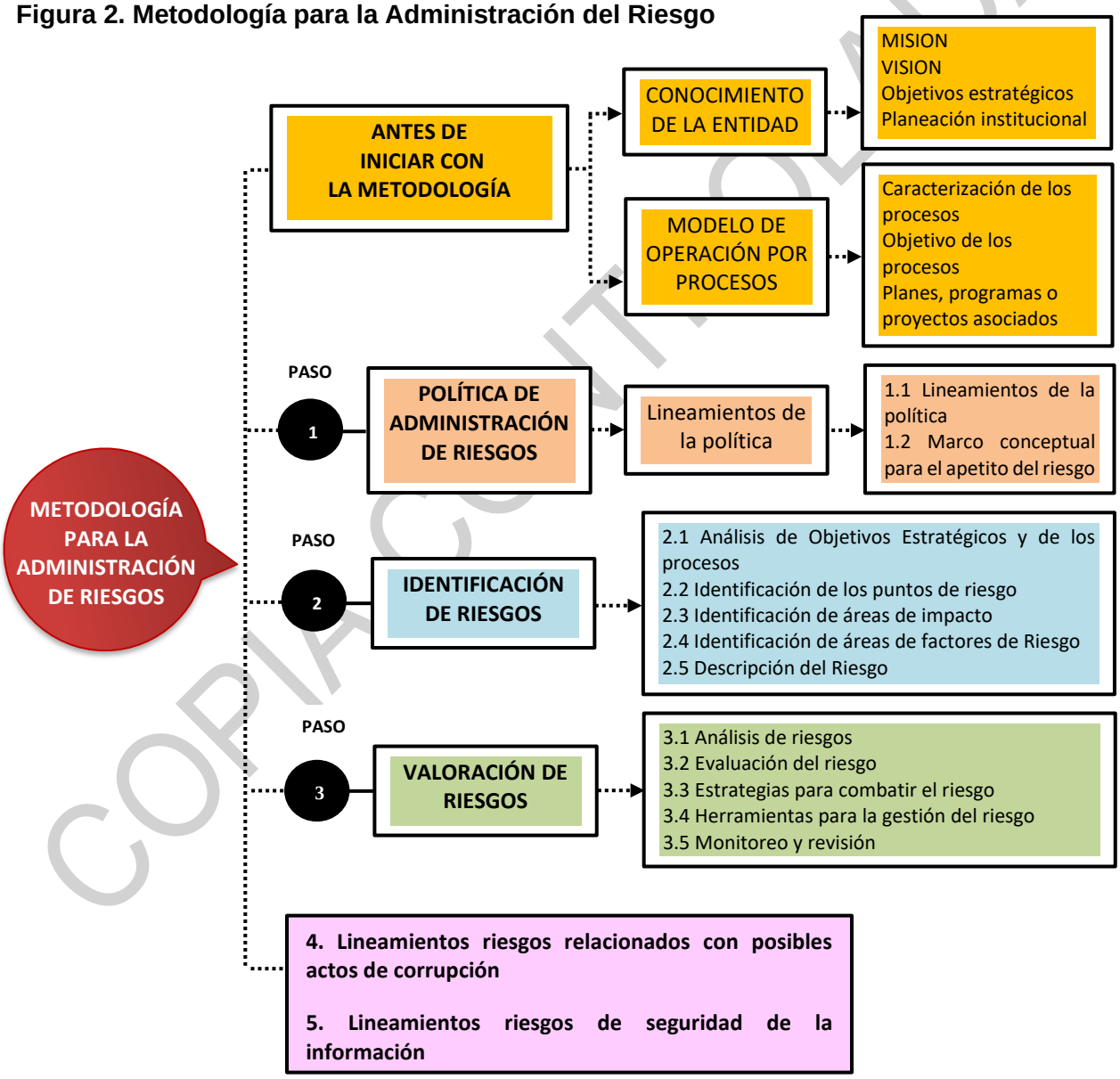
Primera Línea	Líderes de Proceso y equipo de trabajo	• Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera, con énfasis en la prevención del daño antijurídico. • Definir, aplicar y hacer monitoreo a los controles para mitigar los riesgos identificados, alineado con las metas y objetivos de la Entidad y proponer mejoras a la gestión del riesgo en su proceso. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo, 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. • Realizar las acciones necesarias con su respectivo monitoreo, con el fin de evitar la materialización de los riesgos que se encuentren en valoración baja y moderada. • Informar a la Secretaría de Planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. • Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.
Segunda Línea	Secretaría de Planeación y Oficina Asesora TIC´s	**Secretaría de Planeación:** • Asesorar en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración de riesgos institucionales, de corrupción y de seguridad de la información. • Consolidar los Mapas de Riesgos (de gestión, de corrupción) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. • Publicar los mapas de riesgos en la WEB • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de procesos.
		Oficina Asesora TIC´s: • Asesorar a los líderes de proceso en la identificación de los riesgos de seguridad de la información e implementación de los controles definidos. • Presentar al Comité Institucional de Gestión y Desempeño, el seguimiento a la eficacia de los controles de los riesgos de seguridad de la información de los procesos.
Tercera Línea	Oficina de Control Interno de Gestión	• Asesorar y orientar sobre la metodología para la identificación, análisis y valoración del riesgo. • Analizar el diseño e idoneidad de los controles establecidos en los procesos. • Realizar seguimiento a los riesgos consolidados en el mapa de riesgos de gestión (dos veces al año), mapa de riesgos de corrupción (tres veces al año según la norma) de conformidad con el Plan Anual de Auditoría. • Recomendar mejoras a la política de administración del riesgo.

9. METODOLOGÍA PARA LA GESTIÓN 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.

A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Figura 2. Metodología para la Administración del Riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas 2020. Versión 5.

La Alcaldía Municipal para la elaboración del Mapa de Riesgos de Gestión tendrá en cuenta como referente la metodología planteada por el Departamento Administrativo de la Función Pública en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*" de la Función Pública – 2020. Por otra parte, para la construcción del Mapa de Riesgos de Corrupción los lineamientos a aplicar serán los de la Secretaria de Trasparencia de la Presidencia de la Republica de la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*" – versión 4 de 2018.

El resultado de aplicar la metodología propuesta será el Mapa de Riesgos de Gestión y el Mapa de Riesgos de Corrupción, que consolida los riesgos identificados y las acciones que se establezcan para mitigar los mismos, así como los responsables para ejecutarlas.

A continuación, se definen los pasos para la adecuada gestión del riesgo en la Alcaldía de Bucaramanga, que deberán seguir los líderes de los procesos y sus equipos de trabajo, al inicio de cada vigencia**:**

9.1 IDENTIFICACION DE RIESGOS

Para la identificación de los riesgos que están o no bajo el control de la entidad, se debe tener en cuenta el contexto estratégico en el que opera la alcaldía de Bucaramanga, la caracterización de cada proceso que contempla su objetivo y alcance, Interrelación con otros procesos, Procedimientos asociados, Responsables del proceso y Comunicación entre los procesos. Además, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

De acuerdo con la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se identifican riesgos de proceso, corrupción y de seguridad de la información

La totalidad de riesgos que se identifiquen en el mapa de riesgos de cada proceso estarán sujetos al monitoreo, ajuste, control y seguimiento por parte de los líderes y su equipo de trabajo; lo cual incluye acciones que permitan combatir el riesgo para Reducirlo, Aceptarlo o Evitarlo y ser tratados al interior de cada proceso de acuerdo con la severidad del riesgo para Transferirlo o Mitigarlo.

En el caso de los riesgos de corrupción, estos no admiten aceptación del riesgo, por lo cual siempre deben tener un tratamiento con acciones precisas.

9.1.1 Análisis de Objetivos Estratégicos y de los Procesos. Este análisis es importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico (Misión y Visión) o del proceso (estén alineados con la Misión y Visión y contribuya al cumplimiento del objetivo estratégico).

En cada vigencia se analizará el entorno estratégico de la entidad a partir de algunos factores internos y externos, para el adecuado análisis de las causas del riesgo y gestión de éste, se tendrá una guía específica de Contexto Organizacional diseñada por la institución, "Guía para la identificación del Contexto Organizacional" código G-DPM-1210-170-001, el formato Contexto Estratégico código F-DPM-1210-238,37-014 y el formato Mapa Riesgos de Gestión código F-DPM-1210-238,37-013.

Tabla 2. Análisis Objetivos estratégicos y de los procesos

Análisis de objetivos estratégicos y de los procesos	
CONTEXTO EXTERNO	Económicos (Disponibilidad de capital, liquidez, mercados, financieros, desempleo, competencia)
	Políticos (Cambios de gobierno, legislación, políticas públicas, regulación)
	Sociales (Demografía, responsabilidad social, orden público)
	Tecnológicos (Avances en tecnología, acceso a sistemas de información externos, Gobierno Digital)
	Medio Ambientales (Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible)
	Comunicación externa (Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad).
CONTEXTO INTERNO	Financieros (Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada).
	Personal (Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional).
	Procesos (Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento).
	Tecnología (Integridad y Seguridad de los datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información).
	Estratégicos (Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo).
	Comunicación interna (Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones).
CONTEXTO INTERNO DEL PROCESO	Diseño del proceso (Claridad en la descripción del alcance y objetivo del proceso).
	Interacciones con otros procesos (Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes).
	Procedimientos asociados (Pertinencia en los procedimientos que desarrollan los procesos).
	Responsables del proceso (Grado de autoridad y responsabilidad de los funcionarios frente al proceso).
	Comunicación entre los procesos (Efectividad en los flujos de información determinados en la interacción de los procesos).

9.1.2 Identificación de los Puntos de Riesgo. Son actividades dentro de la cadena de valor (insumos, procesos, productos, resultados e impacto) 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.

Figura 3. Cadena de Valor

Tabla 3. Puntos de riesgos de los procesos

PUNTOS DE RIESGOS DE LOS PROCESOS
1. Operativos: Provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias.
2. Recurso Humano: Se asocian a la cualificación, competencia y disponibilidad de personal requerido para realizar un proyecto o función.
3. Financieros: Relacionados con el manejo de recursos que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes.
4. Cumplimiento y conformidad: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
5.Tecnológicos: Relacionados con la capacidad tecnológica para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
6. De Seguridad de la Información: Se asocia a la disponibilidad, confiabilidad e integridad de la información institucional.
7. De comunicación: Relacionados con los canales, medios y oportunidades para informar durante las diferentes etapas de un proyecto.
8. Contractual: Relacionados con los atrasos o incumplimientos de las etapas contractuales en cada vigencia.

9.1.3 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

Afectación Reputacional: es el deterioro de la relación con los grupos de interés como resultado de una percepción negativa sobre el comportamiento de la empresa.

- Perdidas por la disminución de la confianza en la integridad de la entidad que surge cuando su buen nombre es afectado.
- Opinión publica negativa sobre el servicio prestado.
- La afectación reputacional puede derivar en acciones que fomenten la creación de una mala imagen o un posicionamiento negativo en la mente de los ciudadanos.

Factores:
- Fallas en la comunicación
- Factores externos
- Fallas relevantes en los servicios y productos
- Insatisfacción de los grupos de valor

Afectación económica o presupuestal. Se relaciona con los recursos económicos de la entidad, principalmente de la eficiencia y transparencia en el manejo de los recursos.

Factores:
- Recursos públicos mal utilizados
- Desvío de presupuesto
- Pérdidas por actos de corrupción

9.1.4 Identificación de áreas de Factores de Riesgo. Son las fuentes generadoras de riesgos. En la Tabla 4 encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

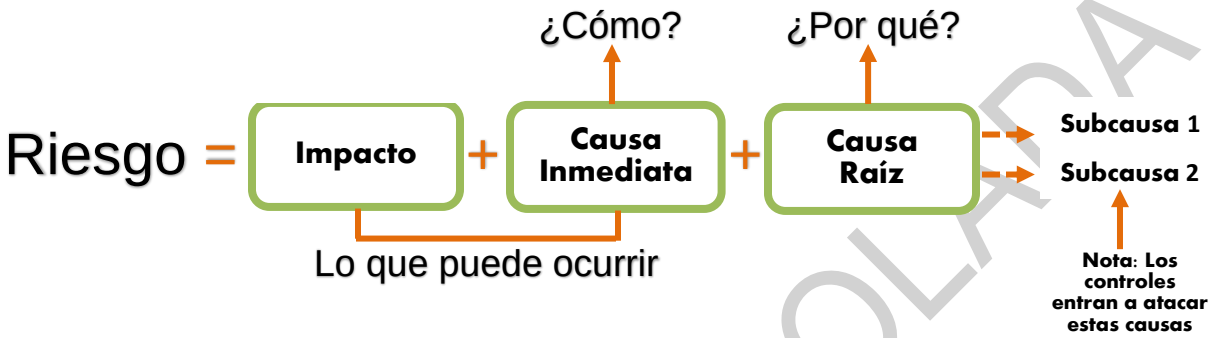
Tabla 4. Factores de riesgo

Factor	Definición	Descripción	
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		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	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto 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
			Accesos no autorizados a información de la entidad
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento Externo	Situaciones externas que afectan la entidad		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas 2020. Versión 5.

9.1.5 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:

Figura 4. Estructura propuesta 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 información es esencial para la definición de controles en la etapa de valoración del riesgo.

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

- **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

- **Causa raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Mediante el análisis de datos históricos, lluvia de ideas, análisis teóricos, opiniones informadas y expertas al interior del equipo de trabajo del proceso, **se analizan las causas inmediatas y las causas raíz** que podrían afectar el cumplimiento del objetivo del proceso, sus posibles efectos, se nombra el riesgo y se clasifica.

A partir de este levantamiento de causas se procederá a **identificar el riesgo**, el cual estará asociado a aquellos eventos o situaciones que pueden afectar económica o reputacionalmente a la entidad.

9.1.6 Clasificación del Riesgo. Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 5. Clasificación y factores de Riesgos

CLASIFICACIÓN	DESCRIPCIÓN	FACTOR DE RIESGO
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	PROCESOS
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	EVENTO EXTERNO
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.	TALENTO HUMANO
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	TECNOLÓGIA
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.	PUEDEN ASOCIARSE A VARIOS FACTORES
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.	INFRAESTRUCTURA
		EVENTO EXTERNO

9.2 VALORACIÓN DE RIESGOS

9.2.1 Análisis de Riesgos. En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

El Riesgo Inherente es el resultado de combinar la probabilidad con el impacto, permite determinar el nivel de riesgo inherente dentro de unas escalas de severidad.

9.2.1.1 Determinar la probabilidad en los Riesgos de Proceso: se entiende como la posibilidad de ocurrencia del riesgo. Es decir, la probabilidad inherente será el **número de veces que se pasa por el punto de riesgo en el periodo de 1 año** y se basa en la **exposición al riesgo** del proceso o actividad que se esté analizando.

De este modo, **la probabilidad analiza la frecuencia con la que se realiza la actividad, y no se basa en eventos**. En la tabla 6 se establecen los criterios para definir el nivel de probabilidad.

Tabla 6. Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 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%

9.2.1.2 Determinar el impacto en los Riesgos de Proceso: Para la construcción de la tabla 7 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, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

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.

Tabla 7. Criterios para definir el nivel de impacto

	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

Ejemplo para la aplicación de la tabla 6 de probabilidad y la tabla 7 de impacto:

	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%

→ La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

	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

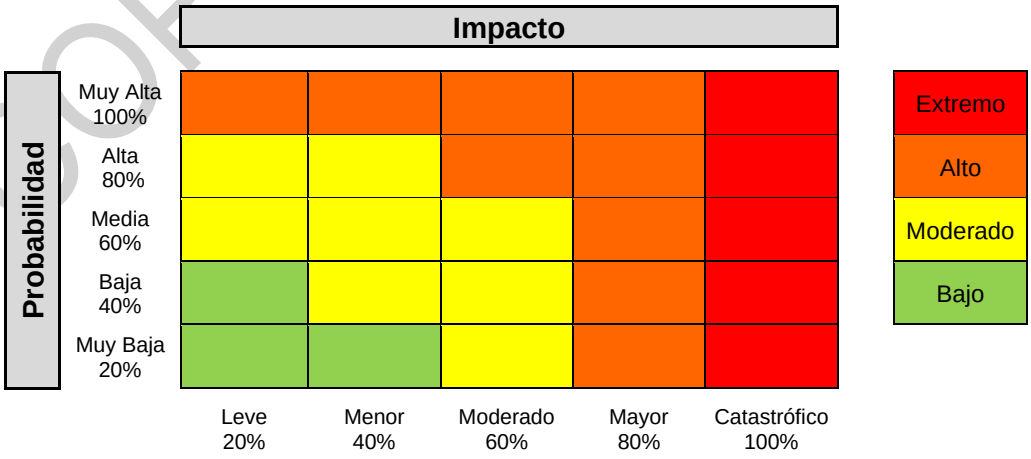
→ La afectación económica se calcula en 500SMLMV, el impacto del riesgo es **mayor.**

De acuerdo con la aplicación de las tablas 6 y 7 para el ejemplo la **Probabilidad inherente =** media 60%, y el **Impacto inherente:** mayor 80%.

9.2.2 Evaluación del Riesgo. 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).

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 (ver figura 5).

Figura 5. Matriz de calor (niveles de severidad del riesgo)



Continuando con el ejemplo donde la **Probabilidad inherente =** media 60%, y el **Impacto inherente:** mayor 80%, se aplica la Matriz de Calor, se tiene:

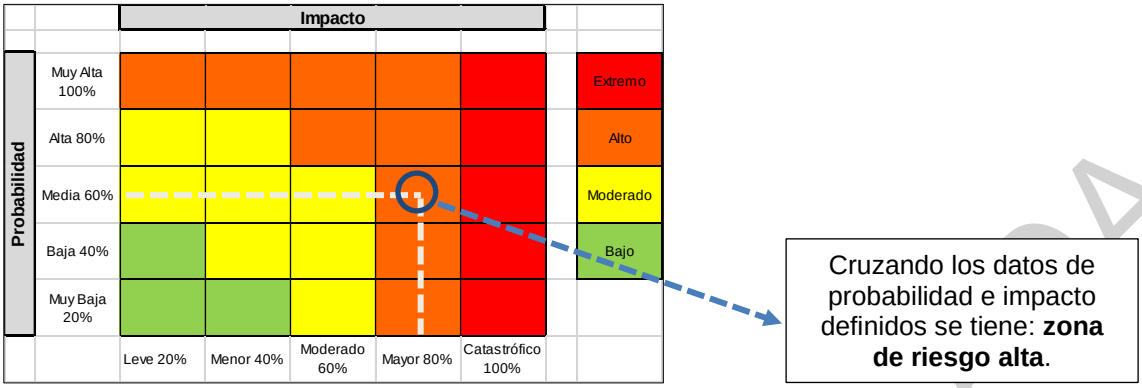


Tabla 8. Matriz Identificación del Riesgo

Paso 1. Identificación del Riesgo												
Proceso:												
Objetivo:												
Alcance:												
Identificación del riesgo												
Referencia	Impacto	Causa Inmediata	Causa Raíz	scripción del Ries	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente

*Nota: La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo con el mismo número. La entidad puede ir en el riesgo 150, pero tener 70 riesgos, lo que permite llevar una traza de los riesgos. Esta información la debe administrar la Secretaría de Planeación o gerencia de riesgos.

9.2.2.1 Valoración de Controles. Conceptualmente 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. En este caso sí aplica el criterio experto.
- **Los responsables** de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.

- **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Tipología de controles y los procesos

Para realizar la **valoración de los controles existentes**, es necesario recordar las siguientes tipologías de controles:

- **Control preventivo (antes):** Acción y/o mecanismo ejecutado 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. Para su identificación se utilizan preguntas como:

  - ¿Están definidos los responsables de la ejecución del control?
  - ¿Está definida la frecuencia de aplicación del control?
  - ¿El control implementado es evidente?
  - ¿El control identificado, ataca por los menos una de las causas generadas identificadas?

- **Control detectivo (durante):** Acción y/o mecanismo que permite detectar el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo. Estos controles detectan el riesgo, pero generan reprocesos.

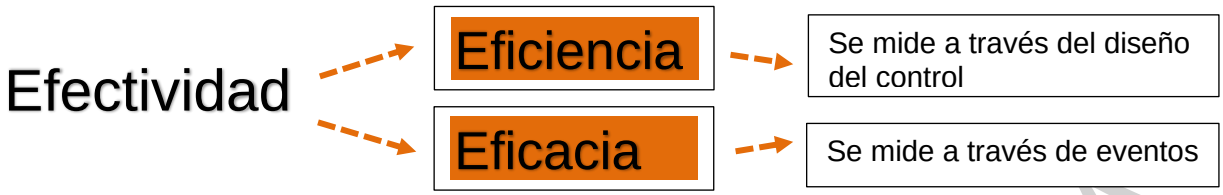
- **Control correctivo (después):** Acción que se ejecuta en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Para su identificación se utilizan preguntas como:

  - ¿Están definidos los responsables de la ejecución del control?
  - ¿Cuenta con planes de contingencia, de acción o alguna directriz documentada que defina los pasos a seguir en caso de materializarse el riesgo?
  - ¿En caso de presentarse el riesgo y de ejecutarse el control, existe alguna manera de evidenciarlo?
  - ¿Cubre por lo menos uno de los efectos del riesgo identificado?

Así mismo, de acuerdo con la forma como se implementan tenemos:

- **Control manual:** controles que son ejecutados por personas, tiene implícito el error humano.
- **Control 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.

Análisis y evaluación de los controles – Atributos: se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.



En la tabla 9 se puede observar la descripción y peso asociados a cada uno así:

Tabla 9. Atributos para el diseño del control

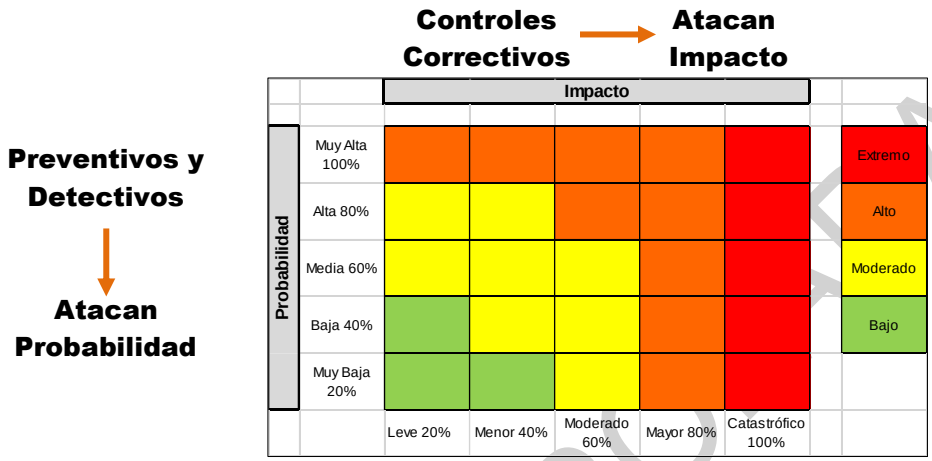
Características de Eficiencia			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado 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 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%
Formalización de Control			**Descripción**	**Peso**
*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:** 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.

Teniendo en cuenta que es a partir de los controles se dará el movimiento en la matriz de calor que corresponde a la figura 6 se muestra cuál es el desplazamiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

De esta manera se identifica si los controles reducen la probabilidad o el impacto, para reducir porcentualmente cada variable.

Figura 6. Desplazamiento en la matriz de calor acorde con el tipo de control



9.2.2.2 Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente y determina el riesgo residual.

Para la aplicación de los controles se debe tener en cuenta que estos **mitigan el riesgo de forma acumulativa**, esto quiere 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**.

- **Riesgo Residual = Riesgo Inherente – (Riesgo Inherente * Control)**

Tiene dos valores, uno de probabilidad y otro de impacto

Si el tipo de control es preventivo o detectivo se desplaza en probabilidad:

- **Probabilidad Residual = Probabilidad Inherente – (Probabilidad Inherente * Control)**

Si el tipo de control es correctivo se desplaza en impacto:

- **Impacto Residual = Impacto Inherente – (Impacto Inherente * Control)**

Dependiendo del nivel de severidad en que se ubique el riesgo residual, la entidad podrá priorizar la atención de estos, así como definir su tratamiento y las acciones a seguir.

Ejemplo:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2%**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Nota: La entidad deberá implementar en el marco de su gestión del riesgo una política de reducción máximo del 50%, para evitar que un solo control baje mucho el nivel del riesgo (ejemplo: Control = preventivo (49%) + automático (49%) = 98%).

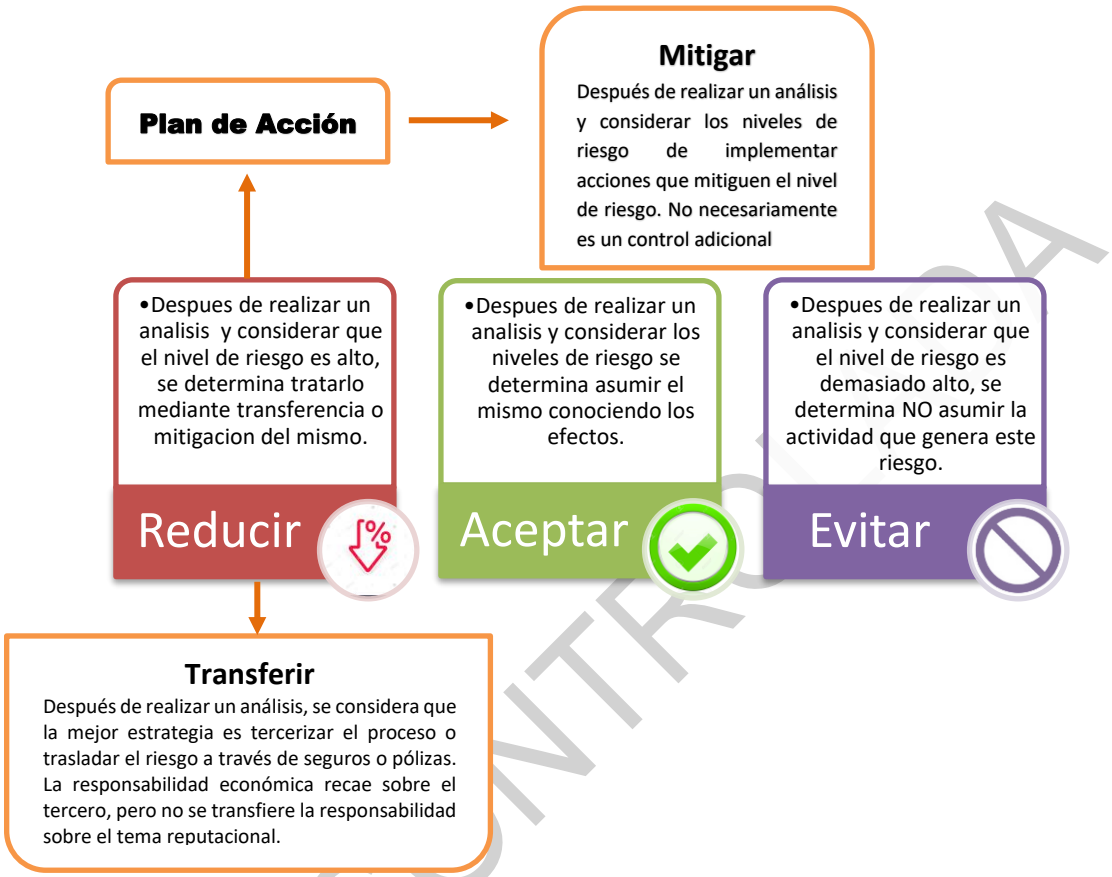
Tabla 10. Matriz Valoración del Riesgo

Paso 2. Valoración del Riesgo															
Evaluación del riesgo - Valoración de los controles									Evaluación del riesgo - Nivel del riesgo residual						
No. Control	Descripción del Control	Afectación	Atributos						Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Fina	Tratamiento
			Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
1															
2															

9.2.3 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 7 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Figura 7. Estrategias para combatir el riesgo



Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

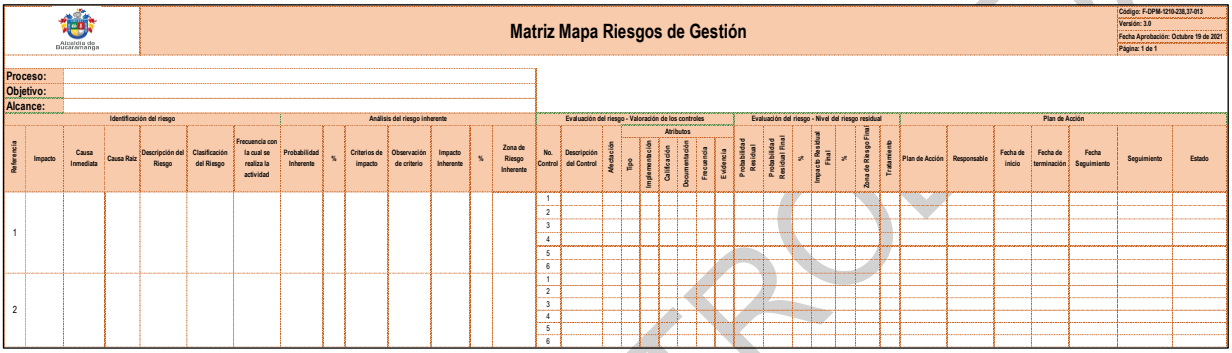
Tabla 11. Plan de acción (para la opción de tratamiento reducir)

Paso 3. Plan de Acción						
Plan de Acción						
Plan de Acción	Responsable	Fecha de inicio	Fecha de terminación	Fecha Seguimiento	Seguimiento	Estado

9.2.4 Herramientas para la gestión del riesgo: como producto de la aplicación de la metodología se contará con la siguiente herramienta: **MATRIZ MAPA RIESGOS DE GESTIÓN** F-DPM-1210-238,37-013 – Donde se consolida la probabilidad e impacto de uno o más riesgos frente a un proceso.

Se identifican las acciones a emprender durante cada vigencia para la adecuada administración del riesgo, se determina el responsable de cada una de ellas y la evidencia que quedará de dicha actividad, se documenta en el **Mapa Riesgos de Gestión** por proceso:

Tabla 12. Matriz Mapa Riesgos de Gestión



Matriz Mapa Riesgos de Gestión

Código: F-DPM-1210-238,37-013 | Versión: 3.0 | Fecha Aprobación: Octubre 19 de 2021 | Página: 1 de 1

Proceso:
Objetivo:
Alcance:

Identificación del riesgo							Análisis del riesgo inherente						Evaluación del riesgo - Valoración de los controles								Evaluación del riesgo - Nivel del riesgo residual							Plan de Acción					
Referencia	Impacto	Causa Inmediata	Causa Raiz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Observación de criterio	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Atributos					Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha de inicio	Fecha de terminación	Fecha Seguimiento	Seguimiento	Estado
																	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia												
1														1																				
														2																				
														3																				
														4																				
														5																				
														6																				
2														1																				
														2																				
														3																				
														4																				
														5																				
														6																				

La Secretaría de Planeación publicará los mapas de riesgos por proceso en la página web Institucional. Posterior a su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el documento. En este caso deberá dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

9.2.5 Monitoreo y Revisión: Los líderes de proceso en conjunto con su equipo de trabajo deben registrar los avances en el mapa de riesgos y analizar el estado de sus procesos frente a los controles establecidos.

En esta fase se debe:

a) Garantizar que los controles son eficaces y eficientes.
b) Obtener información adicional que permita mejorar la valoración del riesgo.
c) Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
d) Detectar cambios en el contexto interno y externo.
e) Identificar riesgos emergentes.

Nota: El monitoreo y revisión permite determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los factores de riesgo, así como su identificación, análisis y valoración.

a. Monitoreo y revisión:

- ✓ Primera Línea de Defensa: Los líderes de proceso con su equipo deben monitorear y revisar periódicamente el mapa de riesgos de gestión, con el fin de asegurar que las acciones establecidas se están llevando a cabo y evaluar la eficacia en su implementación, para evidenciar aquellas situaciones que pueden influir en la aplicación de acciones preventivas.
- ✓ Segunda Línea de Defensa: Monitorear los controles establecidos por la primera línea de

defensa acorde con la información suministrada por los responsables de procesos.

b. Seguimiento:

- ✓ Tercera Línea de Defensa: La Oficina de Control Interno de Gestión, es la encargada de adelantar el seguimiento a los riesgos consolidados en el Mapa de Riesgos de Gestión (dos veces al año). Para tal efecto, los responsables de cada proceso deben aportar los soportes y registros que validen el avance en la ejecución de las acciones propuestas.

9.2.6 Periodicidad. La actualización del Mapa de Riesgos de Gestión y del Mapa de Riesgos de Corrupción del Municipio de Bucaramanga, se realizará como mínimo una vez al año durante el primer trimestre de la vigencia o cuando las circunstancias lo ameriten, a partir de modificaciones o cambios relevantes en los procesos, o cualquier hecho externo e interno que afecte la operación de la entidad.

9.3 LINEAMIENTOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

En materia de riesgos asociados a posibles actos de corrupción, se consideran los siguientes aspectos:

- El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

9.3.1 Identificación del riesgo de corrupción.

9.3.1.1 Procesos, procedimientos o actividades susceptibles de riesgos de corrupción. A manera de ilustración a continuación se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos:

Tabla 13. Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

Direccionamiento estratégico (alta dirección)	• Concentración de autoridad o exceso de poder. Extralimitación de funciones. • Ausencia de canales de comunicación. • Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	• Inclusión de gastos no autorizados. • Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. • Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. • Inexistencia de archivos contables. • Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	• Estudios previos o de factibilidad deficientes. • Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). • Pliegos de condiciones hechos a la medida de una firma en particular. • Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). • Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. • Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. • Urgencia manifiesta inexistente. • Concentrar las labores de supervisión en poco personal. • Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	• Ausencia o debilidad de medidas y/o políticas de conflictos de interés. • Concentración de información de determinadas actividades o procesos en una persona. • Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. • Ocultar la información considerada pública para los usuarios. • Ausencia o debilidad de canales de comunicación
De Investigación y Sanción	• Ausencia o debilidad de medidas y/o políticas de conflictos de interés. • Concentración de información de determinadas actividades o procesos en una persona. • Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. • Ocultar la información considerada pública para los usuarios. • Ausencia o debilidad de canales de comunicación
De trámites y/o servicios internos y externos	• Cobros asociados al trámite. • Influencia de tramitadores. • Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	• Falta de procedimientos claros para el trámite • Imposibilitar el otorgamiento de una licencia o permiso. • Tráfico de influencias: (amiguismo, persona influyente).

9.3.1.2 Lineamientos para la identificación del riesgo de corrupción

Las preguntas clave para la identificación del riesgo son:

¿Qué puede suceder?
¿Cómo puede suceder?
¿Cuándo puede suceder?
¿Qué consecuencias tendría su materialización?

Figura 8. Descripción del riesgo de corrupción

RIESGO DE CORRUPCIÓN
Definición de Riesgo de corrupción: **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. *"Esto aplica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes No. 167 de 2013).* Es necesario que en la descripción del riesgo concurran los **componentes de su definición** así: **▪ ACCIÓN U OMISION** **▪ USO DEL PODER** **▪ DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO** **▪ EL BENEFICIO PRIVADO**

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción porque incorpora cada uno de los componentes de su definición.

Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

Tabla 14. Matriz para la definición del riesgo de corrupción

Matriz definición del riesgo de corrupción				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo publico**	**Beneficio privado**
Riesgo 1	**X**	**X**	**X**	**X**

9.3.2 Valoración del riesgo. Consiste en establecer 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).

9.3.2.1 Determinación de la probabilidad. Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad:

FRECUENCIA	FACTIBILIDAD
Bajo el criterio de FRECUENCIA se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.	Bajo el criterio de FACTIBILIDAD se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Para su determinación se utiliza la tabla de criterios para calificar la probabilidad.

Tabla 15. Criterios para calificar la probabilidad en riesgos de corrupción

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

En caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

Tabla 16. Matriz de priorización de probabilidad

No.	Riesgo	Probabilidad por matriz de priorización	Promedio	Participante 1	Participante 2	Participante 3	Participante 4	Participante 5…
R1								
R2								
R3								

9.3.2.2 Determinación del impacto. Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente 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 establecer estos niveles de impacto se deberán aplicar las siguientes preguntas frente a cada riesgo identificado (ver tabla 17):

Tabla 17. Criterios para calificar el impacto en riesgos de corrupción

No.	PREGUNTA: Si el riesgo de corrupción se materializa podría…	Respuesta	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de la misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicio o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los entes de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinario?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	**¿Ocasionar lesiones físicas o pérdidas de vidas humanas?**		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado		**10**	
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		

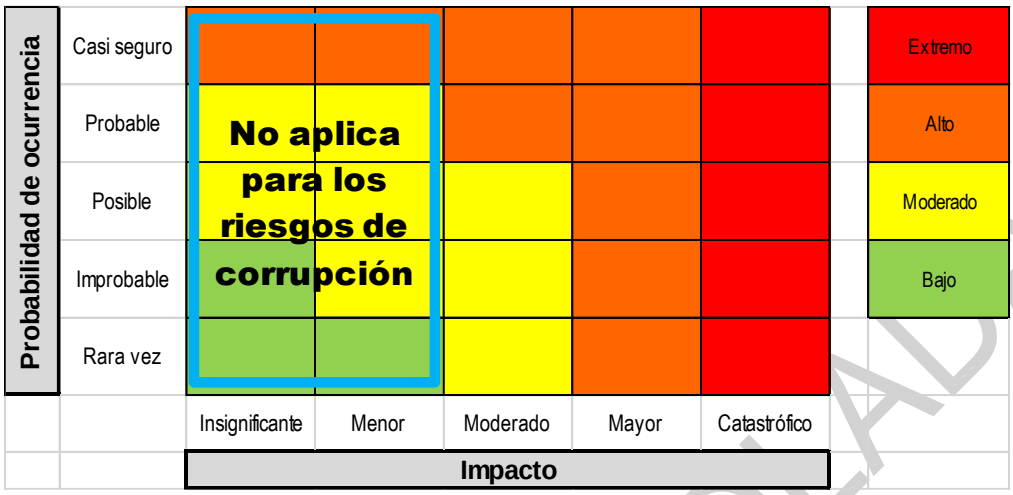
Fuente: Secretaría de Transparencia de la Presidencia de la República.

Observación: Si la respuesta a la pregunta 16 es afirmativa, automáticamente el impacto será **catastrófico.**

9.3.2.3. Análisis del impacto. El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

9.3.2.3.1. Mapa de calor. Se toma la calificación de probabilidad resultante de la tabla "Matriz de priorización de probabilidad", y la calificación de impacto, ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel del riesgo, así se podrá determinar el riesgo inherente.

Figura 9. Matriz de calor para riesgos de corrupción

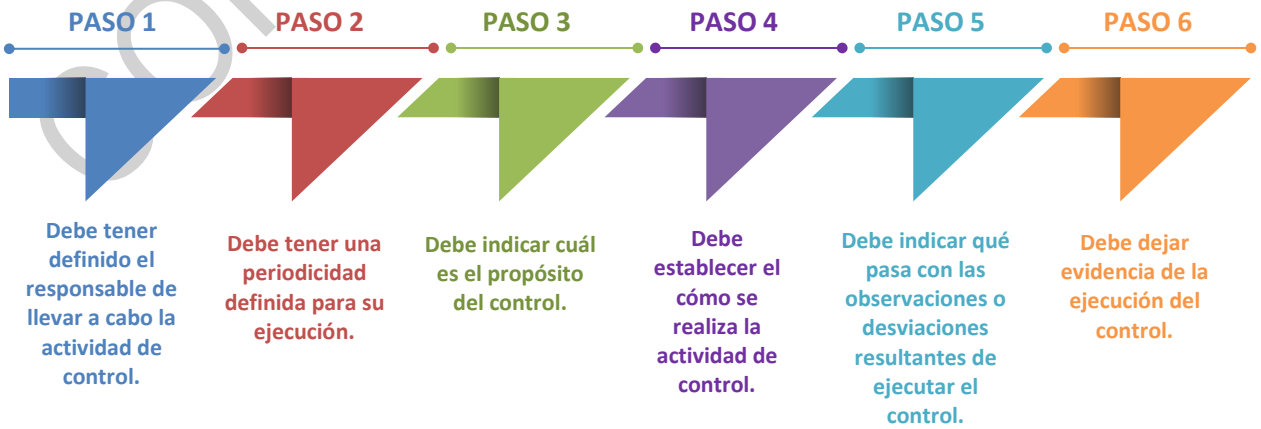


9.3.2.4 Valoración de controles: Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

- Para cada causa debe existir un control.
- Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).
- Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

9.3.2.4.1. Diseño del control: Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo, se deben considerar desde la redacción del mismo, las siguientes variables para la evaluación del diseño del control:

Figura 10. Pasos para diseñar un control



Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

El análisis y evaluación del diseño del control se realiza de acuerdo con las seis (6) variables establecidas:

Tabla 18. Análisis y evaluación de los controles para la mitigación de los riesgos.

CRITERIO DE EVALUACIÓN	ASPECTOS A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No asignado	0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No Confiable	0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente.	0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No existe	0

9.3.2.4.2. Resultados de la evaluación del diseño del control. El resultado de cada variable de diseño (tabla 18), a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

Del mismo modo, aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo, y asegurarse por parte de la primera línea de defensa que el control se ejecute.

Tabla 19. Solidez de controles

Peso del diseño de cada control	Peso de la ejecución del control	Solidez individual de cada control	Debe establecer acciones para fortalecer el control SI / NO
Fuerte Calificación entre 96 y 100	fuerte (se ejecuta de manera consistente).	fuerte + fuerte = fuerte	NO
	moderado (se ejecuta algunas veces)	fuerte + moderado = moderado	SI
	débil (no se ejecuta)	fuerte + débil = débil	SI
Moderado Calificación entre 86 y 95	El control se ejecuta algunas veces por parte del responsable	moderado	SI
Débil Calificación entre 0 y 85	El control no se ejecuta por parte del responsable	débil	SI

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un **Plan de acción** que permita tener un control o controles bien diseñados.

9.3.3. Plan de Acción. Una vez establecida la opción de manejo del riesgo se relacionan las actividades de control, el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer, cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso.

Por último, se formularán los indicadores que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades del control, siempre y cuando conduzcan a la toma de decisiones (por riesgo identificado en los procesos).

Tabla 20. Matriz Plan de Acción Riesgos de Corrupción

Plan de Acción					Observaciones/Desviaciones (Acción de contingencia a implementar si el riesgo se materializa)				Indicador	Monitoreo por parte de segunda línea de defensa o quien haga sus veces	Seguimiento por parte de la Oficina de Control Interno o quien haga sus veces			Estado del plan de acción
Actividad del Control	Soporte	Responsable (Cargo)	Fecha de Inicio	Fecha de Finalización	Acción	Soporte de la acción	Responsable (Cargo)	Tiempo de ejecución (Corto plazo)	Impacto (efectividad, eficiencia)		Seguimiento 1 (Fecha y avance)	Seguimiento 2 (Fecha y avance)	Seguimiento 3 (Fecha y avance)	

9.3.3.1. Monitoreo de riesgos de corrupción. Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa).

Le corresponde, igualmente, a la Secretaría de Planeación adelantar el monitoreo (segunda línea de defensa). Dicho monitoreo se realizará cuatrimestralmente. Su importancia radica en

la necesidad de llevar a cabo un monitoreo constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar. Para tal efecto, deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

9.3.3.2. Seguimiento de riesgos de corrupción. La Oficina de Control Interno, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

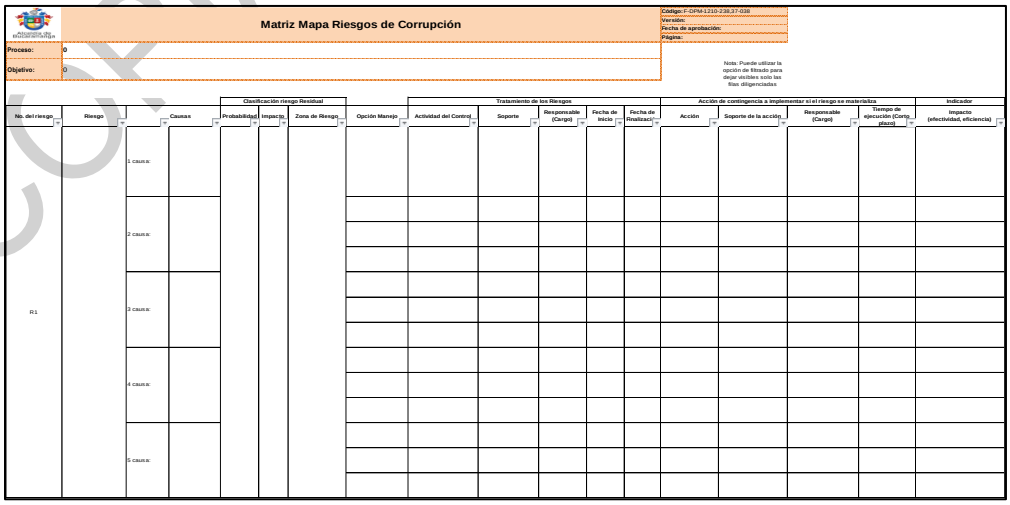
- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

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.

Para la construcción del Mapa de Riesgos de Corrupción incluido en el Plan Anticorrupción y de Atención al Ciudadano – PAAC se realizará teniendo en cuenta la **Matriz Mapa Riesgos de Corrupción F-DPM-1210-238,37-038** de acuerdo con los lineamientos y matriz suministrada por la Secretaría de Transparencia de la Presidencia de la República.

Tabla 21. Matriz Mapa Riesgos de Corrupción



Matriz Mapa Riesgos de Corrupción

Código: F-DPM-1210-238,37-038
Versión:
Fecha de aprobación:
Página:

Proceso: 0
Objetivo: 0

Nota: Puede utilizar la opción de filtrado para dejar visibles solo las filas diligenciadas

				Clasificación riesgo Residual				Tratamiento de los Riesgos					Acción de contingencia a implementar si el riesgo se materializa				Indicador
No. del riesgo	Riesgo		Causas	Probabilidad	Impacto	Zona de Riesgo	Opción Manejo	Actividad del Control	Soporte	Responsable (Cargo)	Fecha de Inicio	Fecha de Finalizaci	Acción	Soporte de la acción	Responsable (Cargo)	Tiempo de ejecución (Corto, plazo)	Impacto (efectividad, eficiencia)
R1		1 causa:															
		2 causa:															
		3 causa:															
		4 causa:															
		5 causa:															

9.3.4 Niveles de aceptación de los riesgos de gestión y de corrupción identificados. La Política de Administración de Riesgos establece las opciones para tratar y manejar los riesgos basada en la valoración de estos, a partir de los criterios ERCA: Evitar, Reducir, Compartir y Asumir.

Por tanto, la entidad establece los siguientes niveles de aceptación y periodicidad de seguimiento a los riesgos identificados (Ver tabla 18)**:**

Tabla 22. Nivel de Aceptación del Riesgo

NIVEL DE ACEPTACIÓN DEL RIESGO
De acuerdo con las responsabilidades establecidas en la presente política, las siguientes acciones estarán a cargo de cada proceso: 1) Cuando al medir la probabilidad e impacto de un riesgo residual de Proceso, éste quede catalogado en **nivel BAJO**, se **ASUMIRÁ el riesgo** y se administrará por medio de las actividades propias del Plan o Proceso asociado y su control y registro de avance se realizará en el documento establecido en el Sistema Integrado de Gestión de Calidad - SIGC. 2) Cuando el nivel del riesgo sea **MODERADO**, se establecerán acciones de Control Preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento **BIMESTRAL** (cada dos meses) y se registrará sus avances en el documento establecido en el SIGC. 3) Cuando el nivel del riesgo residual queda ubicado en la zona de **riesgo ALTA**, se deberá incluir el riesgo en el *Mapa de Riesgos* y se establecerán acciones para abordar los riesgos y las oportunidades que permitan **EVITAR** la materialización de este. La Administración de estos riesgos será con periodicidad **al menos MENSUAL** y su adecuado control se registrará sus avances en el documento establecido en el SIGC. 4) Si el Nivel del riesgo residual se ubica en la zona de **riesgo EXTREMA**, se incluirá el riesgo en el *Mapa de Riesgo* y se establecerán acciones correctivas y preventivas para abordar los riesgos y las oportunidades que permitan **EVITAR** la materialización del riesgo. La Administración de estos riesgos será con periodicidad **mínima MENSUAL** y su adecuado control se registrará sus avances en el documento establecido en el SIGC. ***NOTA:*** Los riesgos de corrupción no admiten aceptación del riesgo, siempre debe conducir a un tratamiento. De igual manera, cuando en el seguimiento periódico que realicen los líderes de proceso a sus respectivos mapas de riesgo se prevea la **materialización del riesgo**, se establecerán **acciones para abordar riesgos** de manera inmediata a través de un Plan de Mejoramiento Institucional, con acciones diferentes a las planificadas inicialmente y se analizará la pertinencia de los controles previamente definidos, asegurando la continuidad del servicio o el restablecimiento de este.

9.4. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

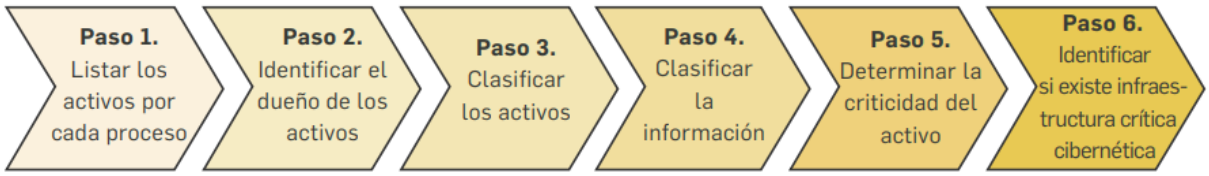
9.4.1 Identificación de activos de información. Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información, son activos de información los elementos que utiliza la entidad para funcionar en el entorno digital y que necesitan ser protegidos, tales como: documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados.

Al identificar los activos también es necesario identificar a sus propietarios, es decir, la persona o unidad organizativa responsable de éste.

De acuerdo con lo anterior, se debe determinar qué es lo más importante que la Administración Municipal y sus procesos poseen (bases de datos, archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios), que permita saber qué es lo que se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Teniendo en cuenta que la Seguridad de la Información debe aplicarse a la totalidad de la operatividad de la entidad, los activos que hacen parte de procesos críticos o misionales estarán clasificados como de mayor importancia y, de acuerdo con el proceso, los demás activos tendrán asignado un nivel de criticidad en cuanto a la información que contienen o gestionan.

La identificación y valoración de activos debe ser realizada por los Líderes de Proceso (primera línea de defensa) en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de Seguridad de la información de la Administración Municipal, con los siguientes pasos:



Paso 1. Listar los activos por cada proceso. En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Paso 2. Identificar el dueño de los activos. Cada uno de los activos identificados deberá tener un propietario designado, Si un activo no posee un propietario, nadie se hará responsable ni lo protegerá debidamente.

Paso 3. Clasificar los activos. Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red, entre otros.

Paso 4. Clasificar la información. Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su

Guía No.5 de Gestión y Clasificación de Activos, el Dominio 8 (Gestión de Activos) del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.

Paso 5. Determinar la criticidad del activo. La entidad debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno para posteriormente, durante el análisis de riesgos, tener presente esta criticidad y así hacer una valoración adecuada de cada caso.

En este paso se deben definir las escalas de criticidad (ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas. Identificar y reportar a las instancias y autoridades respectivas en el Gobierno nacional si poseen Infraestructuras Críticas Cibernéticas - ICC. Se debe tener en cuenta que el sector Gobierno, al cual pertenece la Alcaldía de Bucaramanga, tiene asignada la escala de valoración de impacto ALTO.

9.4.2 Gestión de Riesgos de Seguridad de la información. La Alcaldía de Bucaramanga designará al responsable de Seguridad de la información, quien deberá cumplir las siguientes responsabilidades respecto a la gestión del riesgo de seguridad de la información:

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

9.4.3 Identificación de los riesgos inherentes de seguridad de la información. Se definen tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, 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.

Los riesgos de seguridad de la información forman parte de los riesgos de proceso, y por tanto se contempla dentro de la metodología descrita en la presente Política de Administración de Riesgos, aplicable a todos los procesos de la Administración Municipal, teniendo en cuenta, además, aspectos descritos en el Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad digital en Entidades Públicas - Guía riesgos 2018.

Los ítems anteriormente mencionados se encuentran alineados con los criterios estipulados en la Política de Seguridad y Privacidad de la Información publicada en la Resolución-0489 del 29 de diciembre de 2017, que es el marco normativo que ha adoptado el municipio para gestionar la toma de decisiones para la Seguridad de Información a través de la articulación de los Sistemas de Gestión de la Administración, implementando políticas, controles y procedimientos que permitan de manera oportuna la atención de riesgos de Seguridad de la Información, así como la buena gestión de la información en el Municipio.

9.4.4. Estimación del Riesgo. Una vez que se han identificado los riesgos, es necesario evaluar el impacto para cada combinación de amenazas y vulnerabilidades de un activo de información específico, en caso de que ello se produzca.

- **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que pasa por el punto del riesgo en un determinado tiempo o que pueda presentarse dicho riesgo. Siguiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, se toma para este criterio como línea tiempo el periodo de un (1) año con los valores recomendados.

  Es importante destacar que la siguiente tabla define la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo de información en cuestión.

Tabla 23. Criterios para definir el nivel de probabilidad Riesgos en activos de información

	Frecuencia de la Actividad	Probabilidad	Relación – Controles
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%	Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección. En el futuro no se esperan incidentes nuevos.
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%	Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección. Es posible la ocurrencia de nuevos incidentes, pero no muy probable.
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%	Los controles de seguridad existentes son bajos o ineficaces. Existe una gran probabilidad de que haya incidentes así en el futuro.
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%	

Tomado y adaptado de Guía para la administración de riesgo y diseño de controles en entidades públicas
Diciembre 2020 – Versión 5

- **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la Alcaldía de Bucaramanga la materialización del riesgo; se refiere a la magnitud de sus efectos. De igual forma y tomando como base la Guía para la administración de riesgo y diseño de controles en entidades públicas y alineándose con estrategia del municipio, se han asumido los criterios y niveles de afectación de acuerdo con dicha tabla:

Tabla 24. Criterios para definir el nivel de Impacto en Riesgos de activos de información

	Afectación económica	Reputacional	Relación – Confidencialidad/Integridad/Disponibilidad
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la entidad.
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	La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la entidad.
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.	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país	

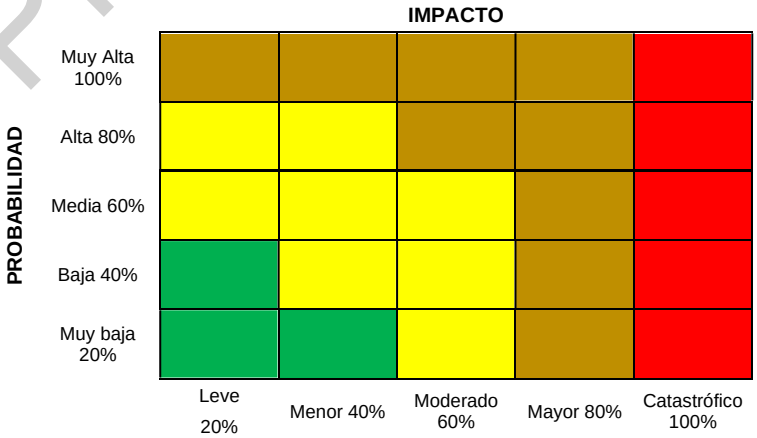
Tomado y adaptado de Guía para la administración de riesgo y diseño de controles en entidades públicas Diciembre 2020 – Versión 5

9.4.5 Determinación del riesgo inherente y residual. De acuerdo plan de tratamiento de riesgos de seguridad digital en el cual se especifica que la exposición al riesgo es la ponderación de la probabilidad e impacto (*Riesgo = Probabilidad * Impacto*).

En la siguiente tabla se muestra la matriz de riesgo, instrumento que muestra las zonas de riesgo y que facilita el análisis gráfico.

Esta herramienta permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados (zona de riesgo **BAJO**, **MODERADO**, **ALTO** o **EXTREMO**) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Figura 11. Matriz de Calor Riesgos de Seguridad de la Información



Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional para la Alcaldía – adaptado del DAFP.

9.5 ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la siguiente tabla:

Tabla 25. Acciones de respuesta a riesgos materializados

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	**Líder de Proceso**	•Informar al Proceso de Planeación y Direccionamiento Estratégico sobre el hecho encontrado. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. • Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Actualizar el mapa de riesgos.
	Oficina de Control Interno de Gestión	• Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos
Riesgos de Gestión y Seguridad de la Información (Zona Extrema, Alta y Moderada)	**Líder de Proceso**	• Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el Plan de mejoramiento. • Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. • Analizar y actualizar el mapa de riesgos. • Informar al Proceso de Planeación y Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas. • Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.
Riesgos de Gestión y Seguridad de la Información (Zona Extrema, Alta y Moderada)	**Oficina de Control Interno de Gestión**	•Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.
Riesgos de Proceso y Seguridad de la Información (Zona Baja)		•Informar al líder del proceso sobre el hecho • Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

Fuente: Política de Operación para la Administración del Riesgo en Función Pública

9.6 DIVULGACIÓN

La Política de Administración de Riesgos, el Mapa de Riesgos de Gestión y el Mapa de Riesgos de Corrupción, se socializarán y divulgarán a todos los servidores públicos de la Alcaldía del Municipio de Bucaramanga, a través de los diferentes medios de comunicación con que cuenta la Entidad.

9.7 CAPACITACIÓN

La Administración del Riesgo se considera un tema de gran importancia para la Administración Municipal. Por ello, se definirán estrategias de capacitación interna y externa que garanticen la competencia necesaria de los servidores para atender el tema de una manera adecuada.

En tal sentido, se requiere que los líderes de proceso fortalezcan el manejo conceptual y operativo en todo lo relacionado con el riesgo.

9.8 REGISTRO DE LA ADMINISTRACIÓN DEL RIESGO

Para garantizar la Trazabilidad de la Administración del Riesgo, el Municipio de Bucaramanga mantendrá registros asociados a los siguientes temas: Monitoreo, seguimiento, ajustes, capacitación, mejora, metodologías, sensibilización y divulgación, lo cual será soportado por la evidencia respectiva.

10. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Original	29 de marzo de 2017
1.0	Se incluyeron los riesgos transversales y códigos de formatos y guía.	30 de mayo de 2017
2.0	Actualización documental, teniendo en cuenta la Guía para la administración del riesgo del DAFP 2018	18 de enero de 2019
3.0	Actualización documental, teniendo en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP 2020.	28 de abril de 2021
4.0	Actualización en los numerales 8. Responsabilidad y Roles – Segunda Línea de Defensa y 9.4 Lineamientos Riesgos de Seguridad de la Información.	03 de agosto de 2021
5.0	Actualización numeral 9.3 lineamientos riesgos relacionados con posibles actos de corrupción, de acuerdo con la Guía para la administración del riesgo del DAFP versión 4 de 2018.	30 de noviembre de 2021