

ALCALDÍA DE PEREIRA



POLÍTICA DE ADMINISTRACIÓN DEL RIESGO ALCALDÍA DE PEREIRA – NIVEL CENTRAL

Junio de 2020

INDICE

INTRODUCCIÓN	3
1. OBJETIVOS.....	4
1.1. Objetivo General	4
1.2. Objetivos Específicos	4
2. ALCANCE	4
3. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS	5
4. PASO A PASO PARA LA ADMINISTRACIÓN DEL RIESGO.....	7
5. ROLES Y RESPONSABILIDADES DE LA ADMINISTRACIÓN DEL RIESGO.	9
6. OPCIONES PARA EL TRATAMIENTO Y MANEJO DEL RIESGO	10
7. PERIODICIDAD PARA EL MONITOREO Y SEGUIMIENTO A LOS RIESGOS	14
7.1. Riesgos de Gestión	14
7.2. Riesgos de Corrupción.....	15
7.3. Riesgos de Seguridad Digital	16
8. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO	17
8.1. Riesgo de Corrupción.....	17
8.2. Riesgos de Gestión y Seguridad Digital	18
9. SOCIALIZACIÓN	18
10. ESTRATEGIAS IMPLEMENTADAS.....	18
11. INTEGRACIÓN DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN CON LA POLÍTICA DE RIESGO.....	19
12. GLOSARIO.....	19

INTRODUCCIÓN

El Departamento Administrativo de la Función Pública, mediante el Decreto 1499 de 2017, determinó que las entidades públicas debían implementar el Modelo Integrado de Planeación y Gestión - MIPG, que integra los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998); que crea un único Sistema de Gestión, articulado con el Sistema de Control Interno (Ley 87 de 1993), el cual se actualiza con el modelo de una línea estratégica y tres líneas de defensa. Lo anterior, con el fin de entregar a los ciudadanos lo mejor de la gestión y, en consecuencia, producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción.

La Alcaldía de Pereira, como entidad pública del Estado, está al servicio de la comunidad. Por lo tanto, es nuestra obligación actuar con transparencia, rectitud e integridad para proteger los activos y recursos que han sido asignados para nuestra debida administración. Es así como se deben tomar todas las medidas necesarias con el objeto de evitar o mitigar cualquier riesgo que se presente en la entidad.

Para ello, se establece que todas las entidades públicas deben contar con una política que facilite la administración de los riesgos, a fin de alcanzar sus objetivos institucionales de manera más eficiente, adelantándose a aquellos eventos que puedan poner en peligro su gestión, por medio del autocontrol y la autoevaluación.

Teniendo en cuenta que la administración de riesgos es estratégica para el logro de los objetivos institucionales y de procesos, en este documento se enuncia la política que permitirá tomar decisiones relativas a la administración de los diferentes riesgos (Gestión, Corrupción y Seguridad Digital), inmersos en el desarrollo de la gestión, lo cual está alineado y armonizado con el Modelo Integrado de Planeación y Gestión MIPG, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, definida por el Departamento Administrativo de la Función Pública - DAFP en versión 4, de octubre de 2018 y articulada con la normativa aplicable a la Entidad.

A través de esta Política, se establecerán los principios necesarios para hacer que la administración y gestión del riesgo sea eficaz, eficiente y coherente, siendo necesario que se implemente en todos los niveles de la Alcaldía de Pereira – Nivel Central, así como en los proyectos y actividades que desarrolla, teniendo siempre en cuenta su contexto, su entorno, sus partes involucradas y la diversidad de criterios de riesgos, entendiendo el riesgo más que como una amenaza, como una

oportunidad de mejora, que bien aprovechada sirve como herramienta para optimizar los resultados.

1. OBJETIVOS

1.1. Objetivo General

Establecer disposiciones y criterios institucionales que orienten a la Alcaldía de Pereira – Nivel Central, en la correcta identificación, análisis, valoración y administración de los riesgos, que pueden afectar el logro de los objetivos institucionales en el marco de los procesos, proyectos y planes, a fin de crear una base confiable que permita tomar decisiones, asignar y utilizar eficientemente los recursos, minimizando los efectos no deseados y buscando la mejora continua en cada uno de los procesos.

1.2. Objetivos Específicos

- Coordinar y realizar las acciones necesarias para reducir vulnerabilidades para prevenir, mitigar, atender y recuperar efectos negativos de posible ocurrencia para la entidad.
- Establecer un mecanismo y periodicidad para la difusión y apropiación de la política de riesgos por parte de toda la entidad.
- Identificar las oportunidades dentro del contexto interno y externo a la Alcaldía de Pereira-Nivel Central que permitan la mejora continua en la gestión.

2. ALCANCE

Los lineamientos presentados en este documento aplican para todos los procesos, subprocesos y dependencias de la Alcaldía de Pereira – Nivel Central, así como a las acciones ejecutadas por los servidores públicos y/o contratistas durante el ejercicio de sus funciones.

Dado que la administración de riesgos de la Alcaldía de Pereira-Nivel Central, tiene un carácter prioritario y estratégico y está fundamentada en la estructura por procesos del Sistema Integrado de Gestión de la Administración Municipal,

establecido en el Decreto 185 de 2017, los pasos de identificación, análisis, valoración, seguimiento y monitoreo de los riesgos de gestión, se ceñirán a los objetivos estratégicos de cada proceso.

3. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

La Alcaldía de Pereira – Nivel Central, tendrá como referencia la “*Guía de Administración del Riesgo y el diseño de controles en entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital*” vigente expedida por el Departamento Administrativo de la Función Pública (DAFP).

La identificación de los riesgos de gestión parte del análisis y la identificación de los objetivos estratégicos de la entidad. En este caso, cada proceso y subproceso cuenta con un objetivo propio de su quehacer, por ello es necesario llevar a cabo una revisión objetiva de la formulación de dichos objetivos, a fin de garantizar que cumplan con los requisitos mínimos, a saber: que sean específicos, medibles, alcanzables, relevantes y proyectados en el tiempo. Deben incluir el qué, cómo, para qué, cuándo y cuánto, ya que, de no estar bien definidos, no se podrá continuar con la metodología de administración de riesgos.

Una vez se tiene definido el objetivo del proceso o subproceso, se procederá con la identificación del riesgo, proceso definido por etapas, como se muestra a continuación:

- **Establecimiento del Contexto:** es la definición de los parámetros internos, y externos que se tomarán en consideración para la administración del riesgo. Para la Alcaldía de Pereira – Nivel Central, se describen así:

Clasificación	Factores
Externos	Económicos: disminución del presupuesto por prioridades del Gobierno, austeridad en el gasto.
	Políticos: cambio de gobierno con nuevos planes y proyectos de desarrollo, falta de continuidad en los programas establecidos, desconocimiento de la Entidad por parte de otros órganos de gobierno, legislación.
	Sociales: ubicación de la Entidad que dificulta el acceso al personal y al público, constantes marchas y paros en el centro de la ciudad.
	Tecnológicos: falta de interoperabilidad con otros sistemas de información, fallas en la infraestructura tecnológica, falta de recursos para el fortalecimiento tecnológico.
	Medio Ambientales: contaminación por sustancias perjudiciales para la salud, malas prácticas de clasificación de residuos.

	<p>Comunicación Externa: múltiples canales e interlocutores de la Entidad con los usuarios, servicio telefónico insuficiente, falta de coordinación de canales y medios.</p> <p>Legal: cambios legales y normativos aplicables a la Entidad y a los procesos</p>
Internos	<p>Financieros: bajo presupuesto de funcionamiento que impide el desarrollo de proyectos, demoras en apropiación y ejecución de recursos, dificultades para la definición de proyectos.</p> <p>Personal: desmotivación de los servidores, falta de incentivos, carrera administrativa sin posibilidades de ascenso, falta de capacitación para desarrollar proyectos, alta rotación, poca apropiación por parte de servidores y contratistas para con MIPG.</p>
	<p>Procesos: incoherencia entre procesos establecidos y ejecutados, desconocimiento de los procesos y procedimientos por parte de los servidores, desactualización de documentos, falta interacción.</p>
	<p>Tecnología: sistemas de gestión ineficientes, falta de optimización de sistemas de gestión, falta de coordinación de necesidades de tecnología.</p>
	<p>Estratégicos: falta de lineamientos y demoras en la Planeación, mapa de procesos desactualizado, estructura organizacional no acordes con procesos, indicadores mal formulados que no aportan a la gestión para toma de decisiones, desconocimiento y falta de aplicación de políticas de operación por parte de los servidores, falta de caracterización de los grupos de valor.</p>
	<p>Comunicación Interna: falta de control sobre los canales establecidos, falta de registros de resultados de reuniones, demoras en bajar la información, poca efectividad en los canales internos,</p>

Fuente: Política de Administración del Riesgo Alcaldía de Pereira – 2019.

De acuerdo con la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se han identificado los siguientes tipos de riesgos al interior de la Administración Municipal – Nivel Central:

- a) **Riesgos de Gestión:** Aquellos riesgos asociados al logro de los objetivos de los procesos institucionales, se identifican y/o validan en cada vigencia por los líderes de proceso y sus respectivos equipos y se clasifican en:

<p>1. Estratégicos: asociado a la administración de la entidad, enfocado a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización por parte de la Alta Dirección.</p>
<p>2. De Imagen: relacionado con la percepción y la confianza por parte de la ciudadanía hacia la Alcaldía de Pereira – Nivel Central.</p>
<p>3. Operativos: comprenden riesgos provenientes del funcionamiento y</p>

operatividad de los sistemas de información institucional, de la definición de los procesos, la estructura de la entidad y la articulación entre dependencias.

4. Financieros: relacionado con el manejo de recursos que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y de los bienes en general.

5. Cumplimiento y conformidad: asociados 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.

6. Tecnológicos: están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

7. De corrupción: relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

8. De Información: se asocia a la calidad, seguridad, oportunidad, pertinencia y confiabilidad de la información agregada y desagregada.

b) **Riesgos de Corrupción:** son los eventos que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, lesionen los intereses de una entidad y en consecuencia, del Estado, para la obtención de un beneficio particular. Se identifican en cada vigencia, junto con los riesgos de gestión, se administran mediante el Mapa de Riesgos Institucional y se determinan acciones preventivas permanentes para evitar su materialización.

c) **Riesgos de Seguridad Digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. Su establecimiento, monitoreo y control son responsabilidad de la Secretaría de las Tecnologías de la Información y las Comunicaciones – TIC y se administran mediante el Mapa de Riesgos de Seguridad Digital Institucional.

4. PASO A PASO PARA LA ADMINISTRACIÓN DEL RIESGO

- **Identificación del Riesgo:** a partir de la determinación del contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos estratégicos.

Las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER?

Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER?

Establecer las causas a partir de los factores determinados en el contexto.

¿CUÁNDO PUEDE SUCEDER?

Determinar de acuerdo con el desarrollo del proceso.

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

Determinar los posibles efectos por la materialización del riesgo.

- Los riesgos, independientemente de su naturaleza, deben estar redactados de una forma clara y precisa, sin dar lugar a ambigüedades o confusiones con su causa generadora.
- Los mapas de riesgos de gestión y de corrupción institucionales, deberán estar publicados en la página web de la Alcaldía de Pereira, a más tardar el 31 de enero de cada año, según la Ley 1474 de 2011 Art 73, Decreto 124 de 2016 y la Ley 1712 de 2014.
- **Redacción del Riesgo:** es importante que, para identificar y redactar el riesgo, se garantice la participación de todos los integrantes del equipo por medio de mesas de trabajo, que faciliten la concertación del mismo y en las que se aproveche el conocimiento y la experiencia, tanto de funcionarios como de contratistas. Se recomienda tener en cuenta los siguientes tips:
 - *Evitar iniciar con palabras negativas, como: “No...”, “Que no...”, o con palabras que denoten un factor de riesgo (causa) tales como “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en...”*
 - *Generar en el lector o escuchala imagen del evento como si ya estuviera sucediendo.*
- **Análisis, Valoración y Tratamiento del Riesgo:** estas etapas se deben adelantar, tomando como base la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 04, de octubre de 2018, diseñada por el Departamento Administrativo de la Función Pública – DAFP, con el acompañamiento de la Oficina de Control Interno.

Desde la Dirección de Sistemas Integrados de Gestión, se ha diseñado un instrumento en formato Excel, que facilita el proceso de identificación, análisis, valoración, tratamiento y seguimiento de los riesgos de gestión, con su respectivo instructivo. Dicha herramienta, se adjunta a este documento. Respecto a los procesos de análisis, valoración y tratamiento de los riesgos de Seguridad Digital, estos serán liderados por la Secretaría de las TIC.

5. ROLES Y RESPONSABILIDADES DE LA ADMINISTRACIÓN DEL RIESGO

Rol	Responsables	Funciones Generales
Línea Estratégica	<p>Alta Dirección</p> <p>Comité Institucional de Coordinación de Control Interno</p>	<p>Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos. Tendrá la responsabilidad de definir el marco general para la gestión del riesgo (Política de Administración del Riesgo) y garantizar el cumplimiento de los planes de la entidad.</p>
Primera Línea	<p>Líderes de procesos y sus equipos</p> <p>Consejo de Gobierno</p>	<p>La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgos y el control sobre una base del día a día.</p> <p>La gestión operacional identifica, evalúa, controla y mitiga los riesgos.</p>
Segunda Línea	<p>Media y Alta Gerencia</p> <p>Comité Institucional de Gestión y Desempeño - CIGD</p>	<p>Asegurar que los controles y procesos de gestión del riesgo de la Primera Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces.</p> <p>Consolidan y analizan información sobre temas claves para la entidad, base para la toma de</p>

		decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
Tercera Línea	Oficina de Control Interno, Auditoría Interna (o quien haga sus veces)	La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporcionará aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y control interno a la Alta Dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.

6. OPCIONES PARA EL TRATAMIENTO Y MANEJO DEL RIESGO

En el tratamiento de los riesgos se tienen todas aquellas estrategias implementadas desde la primera Línea de Defensa para mitigar los diferentes tipos de riesgos que se puedan presentar en la Administración Municipal – Nivel Central.

De esta manera, se establecen las siguientes categorías¹ para su manejo:

a. Aceptar el Riesgo

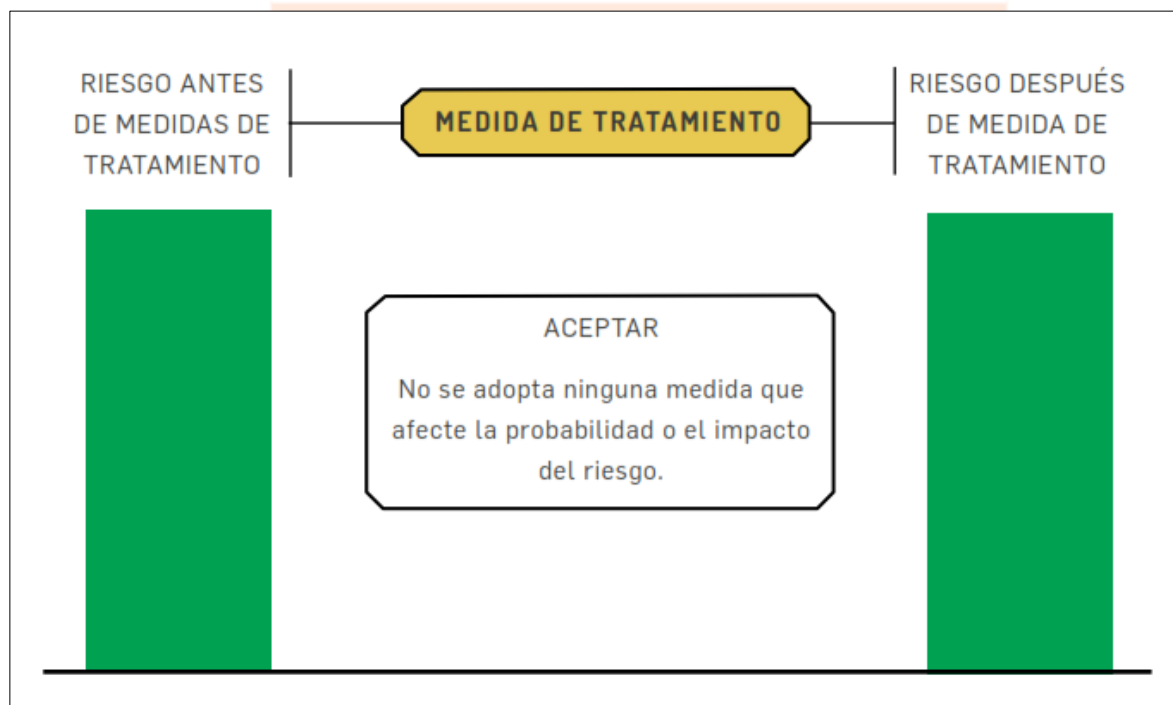
Si el nivel de riesgo cumple con los criterios de aceptación, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

La aceptación del riesgo puede ser una opción viable en la entidad para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

¹Las categorías establecidas para el tratamiento y manejo del riesgo, se determinan según los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP (versión 4, 2018).

Así mismo, como se establece en la guía para la administración del riesgo del DAFP:

- La aceptación del riesgo puede ocurrir sin tratamiento del riesgo.
- Los riesgos aceptados están sujetos a monitoreo.
- No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.
- Los riesgos de corrupción son inaceptables, siempre debe conducir a un tratamiento.
- Los riesgos clasificados en esta categoría, no se incluyen en el mapa de riesgos de gestión.

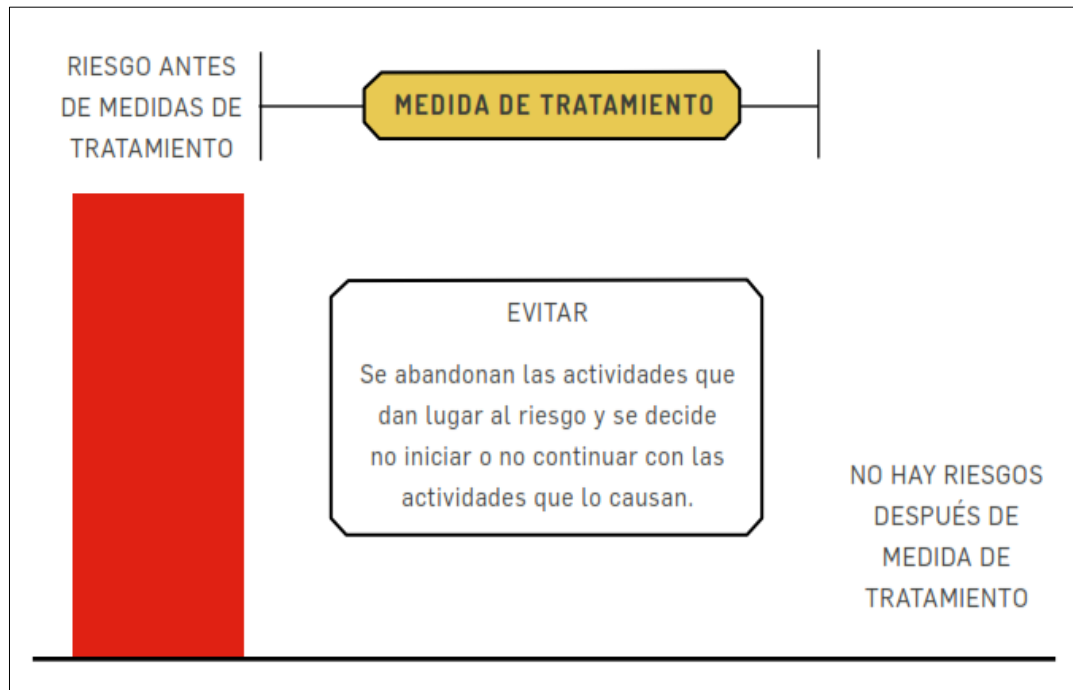


Tomado de “Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP, 2018”

b. Evitar el Riesgo

Cuando los escenarios de riesgo identificados se consideran demasiado extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.

Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.



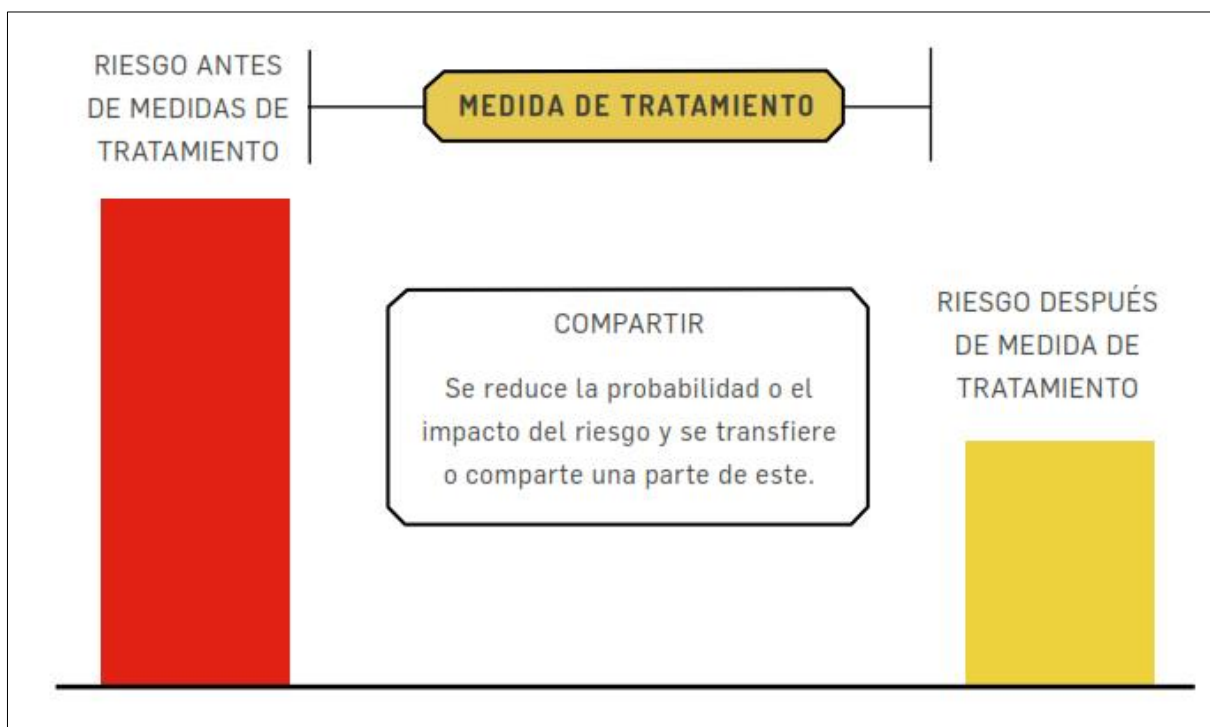
Tomado de “Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP, 2018”

c. Compartir el Riesgo

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

Generalmente, se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de éste. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.



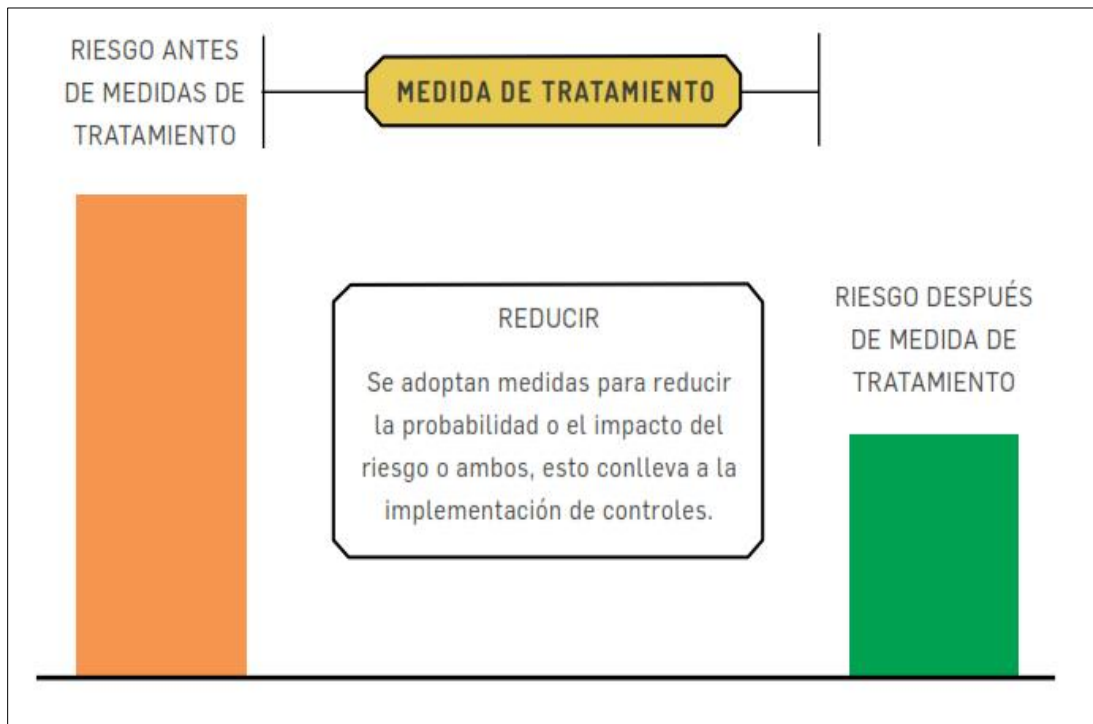
Tomado de “Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP, 2018”

d. Reducir el Riesgo

El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre éste.

Se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambos; por lo general conlleva a la implementación de controles.



Tomado de “Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP, 2018”

7. PERIODICIDAD PARA EL MONITOREO Y SEGUIMIENTO A LOS RIESGOS

7.1. Riesgos de Gestión

- **El Mapa de Riesgo Institucional** estará conformado por los riesgos residuales ubicados en zona de riesgo **ALTA** y **EXTREMA** y el seguimiento y monitoreo lo realizará la Oficina Asesora de Control Interno con periodicidad **SEMESTRAL**.
- Cuando se mide la probabilidad e impacto de un riesgo **INHERENTE** del subproceso y éste queda en zona **BAJA**, se **ACEPTARÁ** el riesgo y se administrará por medio de las actividades propias del subproceso.
- Cuando el nivel del riesgo **RESIDUAL** queda en zona de riesgo **MODERADA**, se deben establecer controles que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se administra mediante seguimiento **SEMESTRAL**, el cual deberá ser reportado a la Dirección de Sistemas Integrados de Gestión - SIG dentro de los primeros 5 días del mes siguiente.

- Cuando el nivel del riesgo residual queda ubicado en la zona de riesgo **ALTA**, se debe incluir el riesgo tanto en el Mapa de Riesgos del subproceso como en el Mapa de Riesgo Institucional y se establecen acciones de control preventivas que permitan **REDUCIR** la materialización del riesgo. La Administración de estos riesgos será con periodicidad sugerida al menos **TRIMESTRAL**, el cual deberá ser reportado a la Dirección de Sistemas Integrados de Gestión - SIG dentro de los primeros 5 días del mes siguiente.
- Si el nivel del riesgo **RESIDUAL** se ubica en la zona de riesgo **EXTREMA**, se incluye el riesgo en el Mapa de Riesgos del subproceso y en el Mapa de Riesgo Institucional, se establecen acciones de control preventivas que tengan viabilidad técnica, financiera, jurídica y relación costo – beneficio, que permitan **EVITAR** la materialización del riesgo, de lo contrario se establecerán acciones preventivas que permitan **REDUCIR** la ocurrencia del riesgo. La Administración de estos riesgos será con periodicidad mínima **TRIMESTRAL**, el cual deberá ser reportado a la Dirección de Sistemas Integrados de Gestión - SIG dentro de los primeros 5 días del mes siguiente de cada proceso.

7.2. Riesgos de Corrupción

- Para **TODOS** los riesgos tipificados como de Corrupción, aunque queden en la zona de riesgo **BAJA**, se establecerán acciones preventivas.
- El seguimiento se realizará con periodicidad **mensual** para evitar a toda costa su materialización por parte de los subprocesos a cargo de los mismos. Su tratamiento será de la siguiente manera:

Zona de Riesgo	Puntaje	Probabilidad	Impacto	Tratamiento
Baja	De 5 a 10 puntos Definida por la casilla Baja	Rara vez o improbable	Moderado y Mayor	Los riesgos de corrupción de las zonas baja se encuentran en un nivel que puede eliminarse o reducirse fácilmente con los controles establecidos en la entidad.
Moderada	De 15 - 25 puntos Definida por la casilla Moderada	Rara vez, Improbable, Posible, Probable y Casi Seguro	Moderado, Mayor y Catastrófico	Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Baja o eliminarlo

Alta	De 30 - 50 puntos Definida por la casilla Alta	Probabilidad: Improbable, Posible, Probable y Casi Seguro	Mayor y Catastrófico	Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Moderada, Baja o eliminarlo
Extrema	De 60 - 100 puntos Definida por la casilla Extrema	Posible, Probable y Casi Seguro	Catastrófico	Los riesgos de corrupción de la Zona de Riesgo Extrema requieren de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección

Nota: en todo caso, se requiere que los subprocesos propendan por eliminar el riesgo de corrupción o por lo menos llevarlo a la Zona de Riesgo Baja.

El seguimiento y monitoreo al mapa de riesgos de corrupción se hará con corte al 30 de abril, 30 de agosto y 30 de diciembre, de acuerdo con la guía "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano - Versión 2" expedida por la Secretaría de Transparencia de la Presidencia de la República, de uso obligatorio para las entidades públicas de acuerdo al Decreto 124 de 2016.

Para llevar a cabo este proceso, los responsables deberán enviar a la Oficina Asesora de Control Interno la información correspondiente en el formato establecido por la GUÍA PARA LA GESTIÓN DE RIESGO DE CORRUPCIÓN, normalizado en la intranet en la ruta *SIG-Formatos de Uso General-Formato de Mapa de Riesgos*, reportando en él el avance en la implementación de las acciones establecidas, a más tardar durante los 5 primeros días hábiles siguientes a estas fechas de corte.

Se subirá el informe de seguimiento en la página web de la Alcaldía de Pereira, <http://pereira.gov.co>, en la ruta *Transparencia-Control-Reportes de Control Interno*, durante los 10 días hábiles siguientes a las fechas enunciadas.

7.3. Riesgos de Seguridad Digital

El proceso de identificación de los riesgos de Seguridad Digital en la Alcaldía de Pereira, se encuentra liderado por la Secretaría de Tecnologías de la Información y las Comunicaciones, quienes son los encargados de determinar la estrategia para la elaboración de los mismos. Sin embargo, contarán con la orientación y acompañamiento de la Dirección de Sistemas Integrados de Gestión – SIG en el desarrollo de dicho tema, dependencia que a su vez facilitará el formato establecido y normalizado para tal fin.

De esta forma, el tratamiento de los riesgos de seguridad digital, comprende por parte de los líderes del proceso, la identificación y determinación de diferentes fases, siendo la Guía para la Administración del Riesgo en las entidades públicas del Departamento Administrativo de la Función Pública – DAFP, el documento metodológico principal para el desarrollo de dicho propósito. El responsable de seguridad digital apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte, como para la gestión y el tratamiento de estos riesgos.

En cuanto a la fase de planificación de los riesgos de seguridad digital, es importante considerar las siguientes actividades:

- Definición del contexto interno, externo y de los procesos de la entidad pública.
- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

Finalmente, cuando se obtenga el mapa de resumen de los riesgos de seguridad digital, éste será presentado por la Secretaría de Tecnologías de la Información y la Comunicación, en el Comité Institucional de Gestión y Desempeño - CIGD, con el fin de que sus integrantes los conozcan y aprueben.

8. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

En el momento que se identifique la materialización del riesgo en la entidad, el líder de la dependencia debe realizar un análisis de las posibles causas del evento y seguidamente efectuar las siguientes acciones:

8.1. Riesgo de Corrupción

- 1) Informar a la Alta Dirección sobre el hecho encontrado.
- 2) Realizar la denuncia ante el ente de control respectivo.
- 3) Iniciar con las acciones correctivas necesarias con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados (plan de mejoramiento).
- 4) Análisis y actualización del mapa de riesgos de corrupción.

8.2. Riesgos de Gestión y Seguridad Digital

- 1) Informar al responsable y líder del proceso sobre el hecho encontrado.
- 2) Tomar las acciones correctivas necesarias, dependiendo del riesgo materializado. (plan de mejoramiento)
- 3) Iniciar el análisis de causas y determinar acciones preventivas y de mejora.
- 4) Analizar y actualizar el mapa de riesgos.
- 5) Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

9. SOCIALIZACIÓN

Es importante socializar los diferentes riesgos (Gestión, Corrupción y Seguridad Digital) encontrados en la entidad con los servidores públicos, antes de publicarlos, por supuesto de manera independiente, porque a pesar de todos ser riesgos, cada uno tiene su tratamiento. Para ello, se debe realizar una serie de actividades, diseñando mecanismos y estrategias para que funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos.

Seguidamente, teniendo un concepto en conjunto con todos los actores inmersos en este proceso, la Política para la Administración del Riesgos de la entidad y el Mapa de Riesgos Institucional (Gestión, Corrupción y Seguridad Digital), se divulgarán a través de Circulares vía SAIA a todos los funcionarios y contratistas de la Administración Municipal – Nivel Central. Así mismo, se publicará en la página web de la Alcaldía de Pereira, a fin de que todas las partes interesadas se informen de la gestión de riesgos realizada por los procesos.

10. ESTRATEGIAS IMPLEMENTADAS

Con el fin de dinamizar el proceso, se realizarán capacitaciones al personal delegado en cada uno de los subprocesos de la entidad, cada vez que se requiera, en cuanto al fortalecimiento y gestión adecuada de los diferentes riesgos (Gestión, Corrupción y Seguridad Digital), teniendo en cuenta la programación de actualización y seguimiento a este tema, por parte de las áreas encargadas.

11. INTEGRACIÓN DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN CON LA POLÍTICA DE RIESGO

La política de administración de riesgos se integra con el Modelo Integrado de Planeación y Gestión - MIPG, a través de la política de Control Interno, pues es allí donde se debe asegurar el cumplimiento de las funciones asignadas, en cuanto a la gestión y el control del riesgo de la Línea Estratégica y las tres Líneas de Defensa establecidas en la entidad, debido a que requiere asegurar el logro de los objetivos propuestos y anticiparse a los eventos negativos, producto de la gestión de la entidad.

12. GLOSARIO

Las siguientes definiciones fueron tomadas de la guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública en su versión 4, en octubre del 2018:

- ✓ **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- ✓ **Amenaza:** situación potencial de un incidente no deseado, el cual puede ocasionar daño aun sistema o a una organización.
- ✓ **Apetito al Riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- ✓ **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- ✓ **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- ✓ **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- ✓ **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- ✓ **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- ✓ **Gestión del Riesgo:** proceso efectuado para proporcionar a la Administración Municipal – Nivel Central, un aseguramiento razonable con respecto al logro de los objetivos.
- ✓ **Impacto:** se entiende como las consecuencias que pueden 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.
- ✓ **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.
- ✓ **Riesgo de Corrupción:** posibilidad que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- ✓ **Riesgo de Gestión:** posibilidad que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- ✓ **Riesgo de Seguridad Digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- ✓ **Riesgo inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la Alta Dirección, para modificar su probabilidad o impacto.
- ✓ **Riesgo residual:** nivel de riesgo permanente, luego de implementar las correspondientes medidas de tratamiento.

- ✓ **Tolerancia al Riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resultan mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- ✓ **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

