ALCALDÍA DE PEREIRA

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO ALCALDÍA DE PEREIRA – NIVEL CENTRAL

Noviembre de 2021

INDICE

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 a través de Modelo Estándar de Control Interno - MECI y el Esquema de 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, obligación de sus servidores públicos y contratistas, actuar con honestidad, respeto, compromiso, diligencia y justicia, para proteger y hacer correcto uso de 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, articulada con la normativa aplicable a la Entidad.

A través de esta Política, se establecen 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 en cuenta su contexto, las partes involucradas y la diversidad de criterios de riesgos, entendiendo el riesgo como una oportunidad de mejora, que bien aprovechada sirve como herramienta para optimizar los resultados, a corto, mediano y largo plazo. En este documento, que contiene la declaración e intención de la Alta Dirección, con

respecto a la gestión del riesgo, se establecen los lineamientos precisos acerca del tratamiento, manejo y seguimiento de los mismos.

El Mapa de riesgos de la Alcaldía de Pereira, está elaborado de acuerdo a los subprocesos contemplados en el Decreto 185 de 2017, “por medio del cual se establece la estructura administrativa de la Administración Municipal”, pero se resalta que cada subproceso es autónomo en la definición e identificación de sus riesgos, así tengan metas y objetivos diferentes.

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, así como 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.

- Desarrollar estrategias que conlleven a un efectivo seguimiento y monitoreo, así como emprender acciones de mitigación de los riesgos.

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 gestión) de cada subproceso.

3. TÉRMINOS Y DEFINICIONES

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 5, de diciembre del 2020:

- ✓ **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 a un sistema o a una organización.

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

- ✓ **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.

- ✓ **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 las cuales se puede presentar el 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.

- ✓ **Nivel de riesgo:** es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo puede ser Probabilidad * Impacto. Sin embargo, pueden relacionarse las variables, a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

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

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

- ✓ **Riesgo residual:** nivel de riesgo permanente, luego de implementar las correspondientes medidas de tratamiento.

- ✓ **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.

- ✓ **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

4. 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"* 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, para ello deben incluir como mínimo el qué, cómo, para qué.

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:

a) ***Identificación de los puntos de riesgo:*** son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Fuente: Política de Administración del Riesgo Alcaldía de Pereira – V3, 2019.

b) ***Identificación de áreas de impacto:*** el área de impacto es la consecuencia **económica** o **reputacional** a la cual se ve expuesta la Administración Municipal – Nivel Central, en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

c) ***Identificación de áreas de factores de riesgo:*** son las fuentes generadoras de riesgos que puede llegar a tener una entidad, tales como:

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
			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 de Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, diciembre 2020.

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.

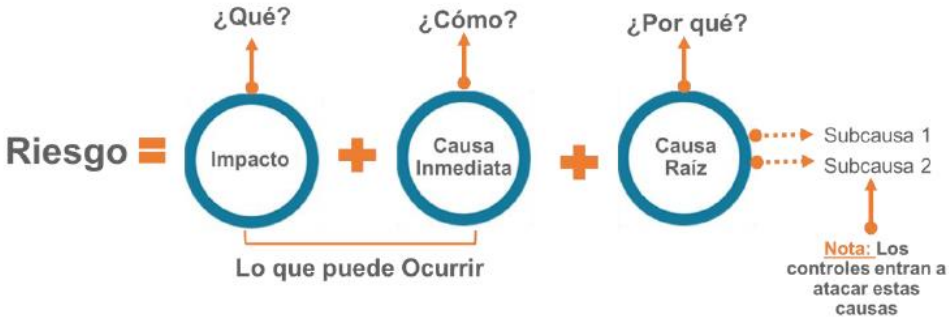
Riesgos de Corrupción: son los eventos que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, lesionen los intereses de una entidad y en consecuencia, del Estado, para la obtención de un beneficio particular. Se identifican en cada vigencia, junto con los riesgos de gestión, se

administran mediante el Mapa de Riesgos Institucional y se determinan acciones preventivas permanentes para evitar su materialización.

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.

5. PASO A PASO PARA LA ADMINISTRACIÓN DEL RIESGO

- ***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 servidores públicos como de contratistas. Se debe tener en cuenta la siguiente estructura:



Fuente: Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, diciembre 2020.

Desglosando dicha estructura, se obtienen los siguientes conceptos:

- **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.

- 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.

- ***Clasificación de los riesgos:***

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5, diciembre 2020.

- ***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 – vigente, diseñada por el Departamento Administrativo de la Función Pública – DAFP. El monitoreo estará bajo la responsabilidad de los líderes de cada uno de los subprocesos que conforman la Administración Municipal – Nivel Central, con el acompañamiento de la Dirección de Sistemas Integrados de Gestión, mientras que el seguimiento será ejecutado desde la Oficina de Control Interno, con la periodicidad que esta dependencia considere.

Desde el Departamento Administrativo de la Función Pública - DAFP, 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, éstos serán liderados por la Secretaría de las TIC.

6. ROLES Y RESPONSABILIDADES DE LA ADMINISTRACIÓN DEL RIESGO

El Modelo de las Líneas de Defensa, en el marco del Modelo Integrado de Planeación y Gestión (MIPG), establece los roles y responsabilidades frente a los diferentes componentes del Sistema de Control Interno. Uno de ellos es la evaluación del riesgo, como proceso dinámico e interactivo que le permite a la entidad identificar, evaluar y gestionar aquellos eventos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales.

La gestión del riesgo en su integralidad, está alineada con la dimensión de Control Interno, que se desarrolla a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en los servidores de la entidad de la siguiente manera:

LÍNEA ESTRATÉGICA

- Define el marco general para la gestión del riesgo y el control.
- Está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.
- Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).
- En consecuencia, tiene la responsabilidad de definir el marco general para la gestión del riesgo y garantiza el cumplimiento de los planes en la entidad.
- Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad.

La línea estratégica o alta dirección debe también asignar entre otros, recursos para garantizar la administración de los riesgos de seguridad digital, tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad digital.

- Recursos económicos para la implementación de controles de mitigación de riesgos (con base al análisis de riesgo realizado).

- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

PRIMERA LÍNEA DE DEFENSA

- A cargo de los gerentes públicos y líderes de los procesos o gerentes operativos de programas y proyectos de la entidad.
- Se encarga del mantenimiento efectivo de controles operativos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.
- Son responsables de implementar acciones correctivas, igualmente detecta las deficiencias de control.
- Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. Implementan procesos para identificar, disuadir y detectar fraudes;

y revisan la exposición de la entidad al fraude con el auditor interno de la entidad.

SEGUNDA LÍNEA DE DEFENSA

- A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de Planeación, coordinadores de equipos de trabajo, comité de enlaces operativos, áreas financieras, área de TIC, entre otros que generen información para el aseguramiento de la operación.
- Asegurar que los controles y procesos de gestión del riesgo de la primera línea de defensa sean apropiados y funcionen efectivamente.
- Ejerce el control y la gestión de riesgos, las funciones de cumplimiento, seguridad, calidad, entre otros.
- Supervisa la implementación de prácticas de gestión de riesgo eficaces por parte de la primera línea y ayuda a los responsables de riesgos a distribuir la información adecuada sobre riesgos a todos los servidores de la entidad.

TERCERA LÍNEA DE DEFENSA

- A cargo de la oficina de Control Interno o quien haga sus veces.
- Proporciona información sobre la efectividad del Sistema de Control Interno, la operación de la primera y segunda línea de defensa con un enfoque basado en riesgos.
- La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporciona aseguramiento 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.
- Coordina la elaboración del mapa de aseguramiento y evalúa la gestión de las segundas líneas de defensa.

Representado de manera gráfica:

ROL	RESPONSABLES	FUNCIONES GENERALES
Línea Estratégica	**Alta Dirección** **Comité Institucional de Coordinación de Control Interno**	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.
Primera Línea	**Líderes de procesos y sus equipos** Consejo de Gobierno	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. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.
Segunda Línea	**Media y Alta Gerencia** (Dentro del Organigrama aquellos cargos que dependen del Representante Legal (Alta Gerencia) Para Media Gerencia, aquellos cargos que se desprenden de los cargos anteriormente mencionados). como por ejemplo jefe de planeación, jefe de contratación, gestión documental, servicio al ciudadano, etc.	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. Consolidan y analizan información sobre temas claves para la entidad, base para la toma de 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 del 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.

7. 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 categorías[1] 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 deberá aplicar para aquellos riesgos residuales ubicados 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.

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

- 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 institucional.

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. **Para el caso de la Alcaldía de Pereira,**

[1]Las 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 5, 2020).

evitar el riesgo no es considerada como una opción de tratamiento a ser implementada.

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.

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. Ésta será la medida de tratamiento del riesgo adoptada en la Administración Municipal – Nivel Central, para aquellos riesgos calificados como altos y extremos.

8. PERIODICIDAD PARA EL MONITOREO Y SEGUIMIENTO A LOS RIESGOS

8.1. Riesgos de Gestión

- **El Mapa de Riesgos 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 **TRIMESTRAL.**

- Cuando se mide la probabilidad e impacto de un riesgo **RESIDUAL** 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.**

8.2. 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

Fuente: Función Pública Guía de Riesgos y Diseño de Controles de Gestión, Corrupción y de Seguridad de la Información, versión 4, de 2018.

Los mapas 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.

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 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 y acceso a la información / 4. Planeación / 4.8 Informes de la Oficina de Control Interno **/** 4.8.2 Otros informes y/o consultas, durante los 10 días hábiles siguientes a las fechas enunciadas.

8.3. Riesgos de Seguridad Digital

El proceso de identificación y monitoreo 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, con la periodicidad que esta dependencia considere. Sin embargo, contarán con la orientación y acompañamiento de la Dirección de Sistemas Integrados de Gestión – SIG en el desarrollo de dicho tema, por medio de la socialización de la metodología establecida por el Departamento Administrativo de la Función Pública – DAFP, vigente, así como de las herramientas sugeridas para ello.

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 y su anexo No. 4, 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.

La gestión de riesgos de seguridad digital para la Alcaldía de Pereira, se realizará a los activos de información que estén clasificados de la siguiente manera:

Categoría: TIC.
Relevancia del activo: Muy importante y Crítico.
Criterios de Confidencialidad, Integridad y Disponibilidad: Alto.

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 lo conozcan y aprueben.

9. 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:

9.1. 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.

9.2. 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.

10. 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 servidores públicos y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos.

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 divulgará, a través de todos los mecanismos oficiales de comunicación habilitados en la Administración Municipal – Nivel Central, para tal fin. Así mismo, se publicará en la página web de la Alcaldía de Pereira, para que todas las partes interesadas se informen de la gestión de riesgos realizada por los subprocesos.

11. ESTRATEGIAS IMPLEMENTADAS

Con el fin de dinamizar el proceso, se realizarán capacitaciones al personal delegado en cada uno de los subprocesos de la entidad, con la periodicidad requerida por cada uno de ellos, 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.

12. INTEGRACIÓN DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN CON LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DE LA ALCALDÍA DE PEREIRA

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. Así mismo, a través de la política de Direccionamiento Estratégico y Planeación, puesto que se hace necesario emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.