POLÍTICA DISTRITAL DE ADMINISTRACIÓN DE RIESGOS

ALCALDÍA MAYOR DE CARTAGENA DE INDIAS

Direccionamiento Estratégico

2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El MIPG opera a través de la puesta en marcha de 7 dimensiones, estas dimensiones recogen los aspectos más importantes de las prácticas y procesos que adelanta la entidad para transformar insumos en resultados que produzcan los impactos deseados, esto es, una gestión y un desempeño institucional que generan valor público, y en procura de un mejoramiento continuo y de la salvaguarda de los recursos, se debe establecer políticas, métodos, procedimientos y mecanismos de prevención, evaluación y seguimiento efectivo a los riesgos de gestión y corrupción, así como la implementación de las acciones de mitigación.

La Política de Planeación institucional tiene como propósito permitir que las entidades definan la ruta estratégica y operativa que guiará la gestión de la entidad, con miras a satisfacer las necesidades de sus grupos de valor.

La administración del Riesgo comprende el conjunto de Elementos de Control y sus Interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales; contribuye a que la entidad consolide su Sistema de Control Interno y a generar una cultura de Autocontrol y autoevaluación al interior de esta.

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 marco de acción que permitirá tomar decisiones relativas a la administración del riesgo el cual está alineado con : el Modelo Integrado de Planeación y Gestión MIPG, la Guía para la Gestión del Riesgo establecida por el Departamento Administrativo de la Función Pública Vigente y el manual para la identificación y cobertura del riesgo en los procesos de contratación.

Así mismo, la presente política involucra, mediante un ámbito estratégico y tres líneas de defensa, a todos los servidores de la entidad, soportándose en los mecanismos de comunicación disponibles, y cubriendo todas las responsabilidades institucionales, las

de cada proceso y las propias de cada servidor. Los niveles de aceptación de riesgo, los ciclos de establecimiento y seguimiento, los niveles de calificación, la identificación de riesgos estratégicos, operacionales, de corrupción y los de contratación, entre otros, hacen parte fundamental del lenguaje y herramientas disponibles para la administración de riesgos.

Cabe resaltar que esta política en su diseño contempla la administración de otras tipologías de riesgos correspondientes a los sistemas de gestión ya implementados en la Alcaldía Mayor de Cartagena de Indias.

2. OBJETIVO

Definir los lineamientos y criterios para orientar a la Alcaldía Distrital de Cartagena de Indias D.T. y C. en la correcta identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos a los que se enfrenta y que puedan afectar el logro de los objetivos institucionales en el marco de los procesos, planes y proyectos de la entidad, así como orientar en las acciones que conduzcan a disminuir la materialización de los riesgos e identificar con mayor precisión las oportunidades de mejora e innovación que se deban emprender para fortalecer la relación ciudadano-Estado.

3. ALCANCE

Esta política aplica al direccionamiento estratégico de la Entidad y se integra a todos los macroprocesos, procesos, subprocesos, planes y proyectos institucionales reflejándose en las acciones ejecutadas por cada servidor público durante el ejercicio de sus funciones; para la correcta gestión de riesgos en el cumplimiento de los objetivos institucionales, orientados en la metodología definida para cada tipología de riesgos de conformidad con la Guía para la administración del riesgo y el diseño de controles en entidades públicas, vigente, publicada por el Departamento Administrativo de la Función Pública.

Adicional a los riesgos de gestión y operativos, es importante identificar los riesgos de corrupción, los riesgos de contratación, los riesgos para la defensa jurídica, los riesgos de seguridad digital, entre otros.

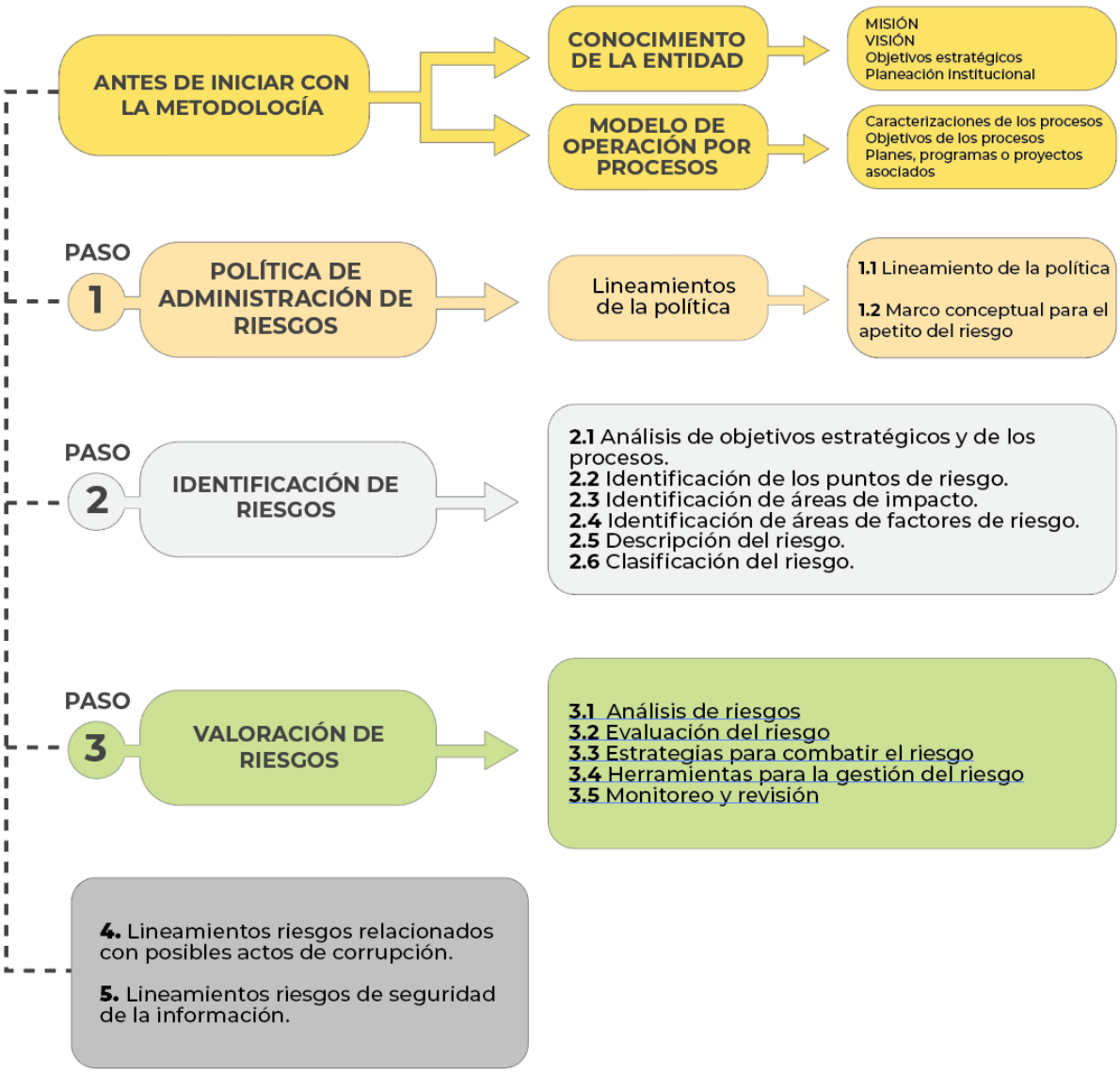
En el caso de los riesgos de seguridad digital, debe ser extensible y aplicable a los procesos de la entidad que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información, habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

4. METODOLOGÍA A UTILIZAR PARA LA GESTIÓN DE LOS RIESGOS

Esta política desarrollará la gestión de riesgos atendiendo los lineamientos fundamentales establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas vigente y expedida por el Departamento Administrativo de la Función Pública DAFP, la cual se entiende integrada a la presente política de administración de riesgos.

La metodología desde un punto de vista estratégico de la aplicación define tres (3) pasos básicos para su desarrollo, como se sintetiza en el siguiente esquema operativo. Para la implantación de la política debe ser comunicada e interiorizada a los servidores públicos de todos los niveles de la entidad, a través de la definición de estrategias de comunicación transversales a la entidad garantizando que su integración en los procesos planes y proyectos sea efectiva. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Metodología para la administración de riesgos



Fuente: Adaptado de Declaración de Posición. Las tres líneas de defensa para una efectiva gestión de riesgo y control.

1. **Esquema tomado de la de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de diciembre de 2020.**

5. DEFINICIONES

- **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.

- **Administración del riesgo:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.

- **Análisis de riesgos:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

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

- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito puede ser diferente para los distintos tipos de riesgo 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 la alta dirección considera que no sea posible el logro de los objetivos de la entidad.

- **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, correspondiente a las razones por las cuales se puede presentar el riesgo.

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

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

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

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

- **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo y su magnitud o ambos son aceptables o tolerables.

- **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.

- **Identificación del riesgo:** Proceso de análisis para encontrar una potencial desviación de los objetivos.

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

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

- **Mapa de calor:** Plano en el que se presentan simultáneamente las escalas de medición de impacto y de probabilidad, y que, como producto de su combinación, mediante colorimetría representa la importancia (nivel de severidad o criticidad) del riesgo.

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

- **Materialización del Riesgo**: Ocurrencia o desarrollo del riesgo

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

- **Objetivo de 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.

- **Oportunidad:** Eventos que permiten alcanzar un resultado esperado o aumentar los efectos deseables.

- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

- **Política de Administración del Riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. 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 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, falla 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 gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- **Riesgo de fraude:** Posibilidad de que la Entidad incurra en una pérdida financiera o de otro tipo cuando una persona (que puede ser empleado, un cliente, o una persona vinculada a la Entidad) que actúa individualmente o en colusión, obtiene una ventaja o beneficio injusto en forma deshonesta o engañosa.

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000). Efecto de la incertidumbre sobre los objetivos. Nota 1 a la entrada: Un efecto es una desviación de lo esperado: positivo o negativo. Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, comprensión o conocimiento de un evento, su consecuencia o probabilidad. Nota 3 a la entrada: El riesgo se caracteriza a menudo por referencia a posibles "eventos" (como se define en la Guía ISO 73: 2009, 3.5.1.3) y "consecuencias" (como se define en la Guía ISO 73: 2009, 3.6.1.3), o una combinación de estos. Nota 4 a la entrada: El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la “probabilidad” asociada (como se define en la Guía ISO 73: 2009, 3.6.1.1) de ocurrencia. Nota 5 a la entrada: En el contexto de los sistemas

de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como efecto de la incertidumbre sobre los objetivos de seguridad de la información. Nota 6 a la entrada: El riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.6

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

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

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

- **Tratamiento del riesgo:** Proceso para modificar el riesgo.

- **Valoración del Riesgo:** Establece la identificación y evaluación de los controles. En la etapa de valoración del riesgo se determina el riesgo residual.

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

2. Las definiciones son tomadas de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020.

6. CONDICIONES

En el presente documento se establecen los siguientes parámetros:

- Los riesgos de gestión se acogen al presente documento.

- Los riesgos de seguridad digital dando cumplimiento a la Política Pública de Tecnologías de la Información y Comunicaciones del Distrito de Cartagena de Indias se acogen al presente documento.

- Los riesgos de gestión en materia de contratación se acogen a las Políticas de Colombia Compra Eficiente.

- Los riesgos de gestión de la operación de los macroprocesos, procesos y subprocesos del sistema integrado de gestión, sistema de gestión de seguridad y salud en el trabajo y sistema de seguridad y privacidad de la información, se acogen al presente documento.

- Los riesgos en materia de seguridad y salud en el trabajo (ocupacionales) dando cumplimiento al Sistema de Gestión de Seguridad y Salud en Trabajo se identifican e implementan de acuerdo con lo establecido en la política de SST.

- Las responsabilidades para la administración del riesgo se definen con base en las líneas de defensa.

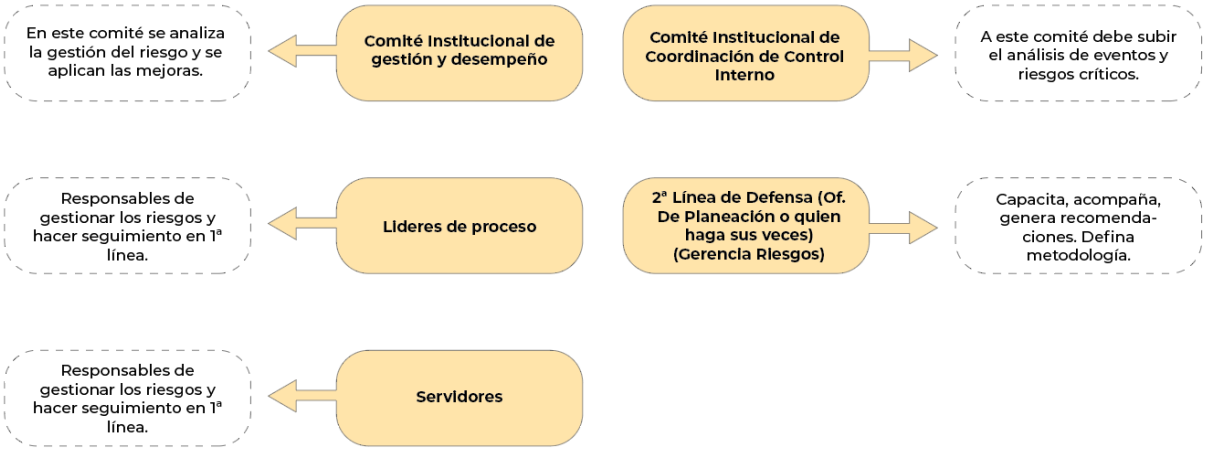
- El Contexto de la Organización (cuestiones internas y externas) se define de acuerdo con las directrices de la Guía metodológica de administración de riesgos y del Modelo integrado de gestión MIPG.

- Las oportunidades se identifican en el Contexto de la Organización, sin embargo, también se pueden identificar en la gestión de los procesos.

7. INSTITUCIONALIDAD

Para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Figura 3 Operatividad Institucional para la Administración del riesgo



8. IDENTIFICACIÓN DE LOS FACTORES DE RIESGO

Desde la perspectiva del contexto estratégico de la Alcaldía Mayor de Cartagena se identificaron algunos factores de riesgo asociados a los respectivos procesos que con su desarrollo contribuirán a dilucidar un análisis de las causas de los riesgos y posteriormente a proyectar la gestión que corresponderá efectuarse en cada caso.

Como referente, a continuación se detallan algunas actividades (que incluye la metodología) relacionadas con la identificación del riesgo:

Tabla 1. Factores de riesgo

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la entidad.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurtos 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 para administración del riesgo y el diseño de controles en entidades públicas, v5. 2020.

Tabla 2. Clasificación de riesgos

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la entidad (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 están involucrado por lo menos 1 participante interno de la entidad, 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 para administración del riesgo y el diseño de controles en entidades públicas, v5. 2020.

Tabla. Actividades relacionadas con la gestión en la Alcaldía Mayor de Cartagena.

Actividad	Frecuencia de la actividad	Probabilidad frente al riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
Tecnología (incluye disponibilidad de aplicativos), tesorería.	Diaria	Muy alta

Fuente: Guía para administración del riesgo y el diseño de controles en entidades públicas, v5. 2020.

Tabla. Criterios para definir el nivel de probabilidad

Nivel	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%

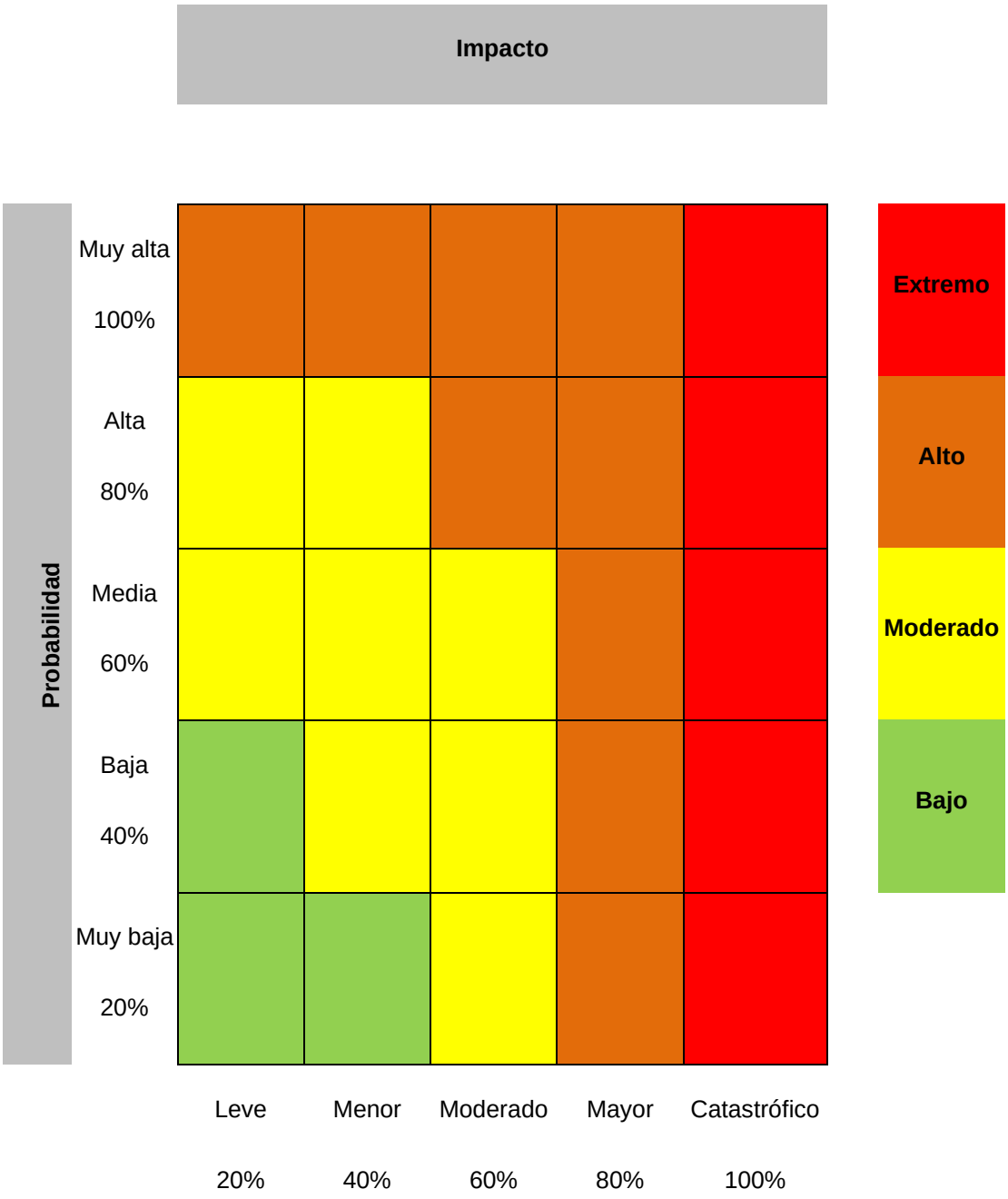
Fuente: Guía para administración del riesgo y el diseño de controles en entidades públicas, v5. 2020.

Tabla. Criterios para definir el nivel de impacto

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

Fuente: Guía para administración del riesgo y el diseño de controles en entidades públicas, v5. 2020.

Matriz de calor (Nivel de severidad del riesgo)



Matriz para la valoración del riesgo

No. control	Descripción del control	Afectación		Atributos						Probabilidad residual (2 [illegible])	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							

Fuente: Guía para administración del riesgo y el diseño de controles en entidades públicas, v5. 2020.

Formato mapa de riesgo. Identificación del riesgo.

Proceso	Gestión de recursos
Objetivo	
Alcance	

Referencia	Impacto	Causa inmediata	Causa raíz	Descripción del riesgo	Clasificación del riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente

Fuente: Guía para administración del riesgo y el diseño de controles en entidades públicas, v5. 2020.

9. NIVELES DE ACEPTACIÓN AL RIESGO.

En relación con el riesgo de corrupción, de ninguna manera será aceptable, sino que se procederá con las acciones de identificación, prevención y control correspondientes en caso de detección, se procederá a efectuar una acción de control y corrección al evidenciarse la materialización del riesgo u ocurrencia del evento, y en esa medida se acudirá a la vía gubernativa respectiva haciendo la denuncia ante las autoridades pertinentes.

En relación con los riesgos de gestión y de seguridad digital identificados en un nivel de impacto BAJO, este se gestionará por medio de las acciones y actividades establecidas en el macroproceso de Gestión tecnología informática y se determinará las acciones de mejora que sean aplicables de acuerdo con los procedimientos asociados y se realizará un reporte bimestral de su desempeño a la Secretaría de Planeación.

Fuente: Adaptado de Declaración de Posición. Las tres líneas de defensa para una efectiva gestión de riesgo y control.

LÍNEA ESTRATÉGICA		
A cargo de la Alta Dirección y Comité Institucional de Coordinación de Control Interno. Esta línea 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 garantiza el cumplimiento de los planes de la entidad.		
1ª LÍNEA DE DEFENSA	**2ª LÍNEA DE DEFENSA**	**3ª LÍNEA DE DEFENSA**
A cargo de los lideres de programas, proceso y proyectos y sus equipos (en general servidores públicos en todos los niveles de la organización)	**A cargo de los lideres de temas transversales estratégicos de gestión, tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, lideres de otros sistemas de gestión, comités de riesgos, entre otros.**	**A cargo de los jefes de control interno o quienes hacen sus veces.**
• Esta línea se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. • Así mismo, identifica, evalúa, controla y mitiga los riesgos.	• Esta línea asegura que los controles y procesos de gestión del riesgo de la primera línea sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgos eficaces. • Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.	• Esta línea ejerce la función de la auditoría interna, a través de un enfoque basado en el riego, 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.

Instituto Internacional de Auditores IIA 2013.

El segundo, una estructura de control basada en el esquema de COSO/INTOSAL, compuesta por cinco componentes, descrito en la gráfica 5

Gráfica. Las líneas de defensa en el modelo estándar de control interno

10. DECLARACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Alcaldía Mayor de Cartagena establece:

Lineamiento 1: Que para todos los sistemas de gestión **y para todo el modelo de operación por procesos**, el pensamiento basado en riesgos debe ser herramienta funcional para el desarrollo de la planeación, el control, la evaluación y la mejora.

Directrices:

1. En la primera línea de defensa, todos los directivos deben fortalecer la cultura de gestión de riesgos en el ámbito institucional, bajo un enfoque estratégico, revisando las necesidades de adaptación al cambio y definiendo o actualizando la política de Administración del Riesgo. Todos los responsables de procesos, programas y proyectos deben gestionar los riesgos a partir del plan de tratamientos definido y su respectivo seguimiento durante la ejecución de las actividades de control, así como la comunicación de los resultados obtenidos y generación de alertas tempranas.

2. En la segunda línea de defensa, todo servidor que tenga rol o funciones de supervisión, control, planeación, seguridad o calidad, debe fortalecer su conocimiento, la verificación y la evaluación de controles en las diferentes tipologías de riesgos y la intensidad y frecuencia de los controles, según corresponda.

   Los líderes responsables de procesos, programas y proyectos deben requerir y compartir la información relacionada con la comunicación y consulta de los seguimientos, el monitoreo, y las estadísticas e indicadores. Toda materialización de riesgos debe ser reportada de inmediato a la Secretaría de Planeación y a la oficina de Control Interno, incluyendo la información y soportes relacionados con el seguimiento a los planes de contingencia realizados.

3. En la tercera línea de defensa, toda auditoría interna debe estar basada en riesgos y debe asegurar la eficacia, mediante la evaluación de la gestión del riesgo y el control interno, incluyendo las maneras en que funcionan las dos primeras líneas de defensa.

Lineamiento 2: Se establece que, el nivel de aceptación del riesgo, una vez se determine su valoración residual, llega hasta la **valoración con nivel bajo**, para todas las tipologías de riesgos identificadas. Por lo anterior, para los casos en que la **valoración residual situé el riesgo en los niveles extremo, alto y moderado**, se deben modificar los controles existentes o generar tratamientos adicionales.

Directrices:

1. En la primera línea de defensa, el equipo directivo, debe evaluar la solidez de los controles existentes para los riesgos estratégicos, después del tratamiento establecido con base en la valoración residual, determinando si se presenta la necesidad de modificar los controles existentes o generar tratamientos adicionales. Todos los responsables de procesos, programas, planes y proyectos deben evaluar la solidez de los controles existentes para cada uno de los riesgos, después del tratamiento establecido con base en la valoración residual, determinando si se presenta la necesidad de modificar los controles existentes o generar tratamientos adicionales.

2. La segunda línea de defensa, todo servidor que tenga rol o funciones de supervisión, control, planeación, seguridad o calidad, es responsable de monitorear la modificación de los controles existentes o la generación tratamientos adicionales, para los riesgos que en su valoración residual se sitúen en los niveles extremo, alto y moderado.

3. La tercera línea de defensa, toda auditoría interna debe estar basada en riesgos y debe evaluar la solidez de los controles existentes, después del tratamiento establecido con base en la valoración residual, exponiendo eventualmente la necesidad de modificar los controles existentes o generar tratamientos adicionales.

Lineamiento 3: **No se admite tolerancia a los riesgos relacionados con prácticas corruptas**. Los riesgos de corrupción gestionados hacen parte del Plan Anticorrupción y Atención al Ciudadano - PAAC.

Directrices:

1. La primera línea de defensa, cada directivo debe reconocer los riesgos que están identificados en el Plan Anticorrupción y Atención al Ciudadano, donde tiene responsabilidad sobre el resultado. Los Directivos se comprometen a fomentar un clima que favorezca el análisis de los riesgos y la implementación de controles y acciones para tratar riesgos y oportunidades que permitan su mitigación y promoción.

   Todos los responsables de procesos, programas y proyectos deben gestionar los riesgos de corrupción: ejecutar los controles, comunicar sus resultados y generar las alertas tempranas que corresponda.

2. La segunda línea de defensa, todo servidor que tenga rol o funciones de supervisión, control, planeación, seguridad o calidad, es responsable de establecer y verificar los controles, en las diferentes acciones comprometidas en el PAAC.

3. La tercera línea de defensa, toda auditoría interna debe estar basada en riesgos y debe asegurar la eficacia, mediante la evaluación de los controles establecidos para los riesgos de corrupción, incluyendo las maneras en que funcionan las líneas de defensa primera y segunda.

   Toda materialización de riesgos debe ser reportada de inmediato a la Secretaria de Planeación y a la Oficina de Control Interno, incluyendo el seguimiento a los planes de tratamiento realizado.

11. ACCIONES PARA LA APROPIACIÓN CULTURAL DE LA GESTIÓN DEL RIESGO

En la Alcaldía Distrital de Cartagena, se promueve la transparencia y se fortalece la cultura de autocontrol y prevención, lo cual contribuye a la administración de riesgos, a través de:

- Capacitaciones para el fortalecimiento conceptual y operativo de la gestión integral

de riesgos, que garanticen la competencia necesaria de los servidores y colaboradores de la Entidad.

- Estrategias de sensibilización y comunicación, que promuevan el pensamiento basado en riesgos.
- Asesorías y acompañamiento para el desarrollo del enfoque de administración de riesgos en las actividades diarias.
- Divulgación de los resultados de la administración y gestión de riesgos en los procesos de la Entidad.
- Seguimiento prioritario a los riesgos ubicados en las zonas de riesgo “extrema” y “alta” de la matriz de riesgos, identificada para cada uno de los procesos de la Entidad.
- Implementar un plan de prevención de riesgos en los procesos de la Entidad.

12. ROLES Y RESPONSABILIDADES

Para la administración integral de riesgos en la Alcaldía Distrital de Cartagena, se determinan los roles de los diferentes actores, teniendo en cuenta las directrices del Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Modelo Integrado de Planeación y Gestión, entre otras, así:

Línea Estratégica - Alta dirección y Comité Institucional de Coordinación de Control Interno, *a quienes corresponde:*

Alta dirección

1. Revisar el contexto estratégico, la plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el propósito de identificar cambios que puedan originar nuevos riesgos o modificar los existentes.

2. Revisar la información de cumplimiento de los objetivos institucionales y de los diferentes procesos, relativa a la implementación de la gestión de riesgos.

3. Analizar el informe de evaluación a la gestión de riesgos y de ser necesario, proponer acciones para mejorar los planes para el tratamiento de los mismos.

4. Asumir la responsabilidad primaria del Sistema de Control Interno y de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo.

Comité Institucional de Coordinación de Control Interno

1. Someter a aprobación del representante legal de la entidad, la política de administración del riesgo.

2. Evaluar y dar lineamientos técnicos sobre la administración de los riesgos de la Entidad.

3. Retroalimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. Así mismo, hacer seguimiento a su administración, gestionar los riesgos estratégicos y aplicar los controles a los mismos.

4. Evaluar los planes de tratamiento establecidos para cada uno de los riesgos materializados, minimizando la posibilidad de que el evento se repita.

Primera Línea – Gerentes públicos y Líderes de procesos en la Alcaldía Distrital de Cartagena, a quienes corresponde con relación a la administración y gestión integral de riesgos las siguientes funciones:

1. Evaluar los cambios que se presenten en el Direccionamiento Estratégico o en el contexto estratégico, y cómo estos cambios originan nuevos riesgos o modifican los existentes.

2. Liderar la identificación de los riesgos del proceso(s) a cargo, teniendo en cuenta las pautas contenidas en el procedimiento de administración de riesgos vigente.

3. Realizar, con el apoyo de su grupo de trabajo, la administración de los riesgos identificados. Así mismo, analizar, calificar, definir controles, realizar acciones y monitoreo según la periodicidad establecida, para su tratamiento y posibles mejoras.

4. Realizar la evaluación de la solidez de los controles, para determinar la pertinencia y la necesidad de ajuste o modificación, en caso de presentarse.

5. Adelantar la revisión, actualización periódica y seguimiento de los mapas de riesgos, en todos aquellos aspectos consignados en el procedimiento y demás directrices frente al tema, y si es el caso ajustarlo, comunicando a la Secretaria de Planeación dichos cambios.

6. Socializar los controles implementados, con el fin de asegurar su comprensión y oportuna aplicación, además de la información necesaria, que dé cuenta de la gestión de los riesgos. Esto se hará de forma constante en los espacios que se determine.

7. Evaluar periódicamente la eficacia de los controles definidos para tratar los riesgos identificados y actualizar tales riesgos, siempre que el proceso fuente de los mismos, tenga cambios en su operatividad.

8. Reportar los planes de tratamiento establecidos para cada uno de los riesgos materializados, incluyendo las actividades para prevenir la no repetición, así como las causas que dieron origen a la materialización de dichos eventos.

De los servidores y servidoras:

1. Participar en la construcción y administración de los riesgos del proceso dentro del cual ejercen sus funciones o desarrollan sus labores.

2. Conocer los riesgos asociados al proceso dentro del cual ejercen sus funciones o desarrollan sus labores, así como los riesgos de la Entidad, con el objeto de identificar los no previstos por los líderes de otros procesos.

3. Identificar, registrar y reportar de manera oportuna riesgos potenciales y/o la posible

materialización de un riesgo identificado, con el objeto de realizar un adecuado tratamiento y/o mitigación de estos.

Segunda Línea – Secretaria de Planeación, Jefe Oficina Asesora Informática, Secretario de Hacienda, Jefe oficina Jurídica, Comité de Contratación, Comité de Conciliaciones, dirección de talento Humano, Servidores responsables de monitoreo y evaluación de controles y Supervisores e interventores a quienes corresponde:

Secretaría de Planeación:

1. Determinar la metodología para la identificación y gestión de riesgos, de acuerdo con la normatividad y los lineamientos establecidos, para cada una de las tipologías de riesgos, a excepción de aquellas tipologías de riesgos que requieren un desarrollo metodológico particular por su naturaleza, tales como: los ambientales, los de seguridad y salud en el trabajo y los de seguridad de la información.

2. Adelantar el monitoreo del mapa de riesgos, evaluando la eficacia en la implementación de los controles y sus acciones, y visibilizando todas aquellas situaciones que dificulten o impidan la administración de los riesgos, en concordancia con la cultura del autocontrol al interior de la Entidad.

3. Formular lineamientos que orienten a los procesos para que se desarrolle de manera eficaz, eficiente y efectiva la gestión de riesgos.

4. Coordinar y dirigir el desarrollo de las etapas previstas para el diseño e implementación del Componente de la administración de riesgos, a través de la herramienta dispuesta para tal fin.

5. Consolidar y publicar el mapa de riesgos institucional.

6. Acompañar y asesorar metodológicamente a los procesos, en la administración y gestión integral de riesgos, en coordinación con la tercera línea de defensa.

Oficina Asesora Informática o de Tecnologías de Información y Comunicaciones: Determinar e implementar la metodología para la identificación y gestión de riesgos de

Activos de Información, de acuerdo con la normatividad y los lineamientos o parámetros establecidos, en particular, para la gestión de esta tipología de riesgos.

Dirección Contractual y Financiera: Determinar e implementar la metodología para la identificación y gestión de riesgos de acuerdo con la normatividad y los lineamientos o parámetros establecidos, en particular, para la gestión de esta tipología de riesgos.

Unidad de Contratación:

1. Revisar que en el estudio previo la tipificación, distribución y asignación de los riesgos previsibles, se haga dentro del marco legal y sin vulnerar derechos de las partes y terceros interesados, y que la modalidad de contratación por la que se opte sea la más conveniente y corresponda al marco de la Ley 1150 de 2007 y sus normas reglamentarias, teniendo en cuenta la justificación contenida en los estudios previos adelantados por la dependencia que necesita la adquisición del bien, servicio u obra.

2. Verificar el comportamiento de los riesgos de cada contrato, cuando se le asigne la supervisión y/o interventoría de alguno, dando especial atención al reporte y seguimiento sobre los eventos que se monitorean, respecto a la parte que le corresponde asumir el riesgo. Cuando se trate de eventos que pudieran impactar el valor del contrato, se dará aviso inmediato al Ordenador del Gasto para la adopción de las medidas que correspondan.

3. Revisar y formular los ajustes necesarios a los procedimientos y manual de riesgos de la contratación y el Comité de Contratación, para aplicar la Política Integral de Administración de Riesgos a todos los procesos de selección y/o contratación.

4. Adoptar, para los riesgos relacionados con la contratación estatal, lo establecido en el Manual para la Identificación y Cobertura de riesgos en los Procesos de Contratación y/o cualquiera que al respecto se genere y /o establezca. Así mismo, los documentos CONPES que el Gobierno Nacional ha adoptado en materia de riesgos contractuales 3186 de 2002 y 3714 de 2011.

Dirección de Talento Humano: Determinar e implementar la metodología para la identificación y gestión de riesgos de Seguridad y Salud en el Trabajo, de acuerdo con la normatividad y los lineamientos establecidos.

Tercera Línea – Oficina de Control Interno, a la cual corresponde:

Oficina de Control Interno:

1. Adelantar el seguimiento a los mapas de riesgos, verificando y evaluando que los líderes de los procesos desarrollen adecuadamente las etapas de identificación, valoración, seguimiento y control de los riesgos identificados, y que adelanten acciones que permitan su administración.

2. Hacer seguimiento a la evolución de los riesgos y al cumplimiento de las acciones propuestas, con el fin de verificar su ejecución, y si es necesario proponer mejoras.

3. Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad.

4. Adelantar el registro de no conformidades, en el marco de las auditorías internas, cuando se constituya un incumplimiento en la aplicación de la política de riesgo, las cuales permiten eliminar la causa que originó dicha situación; de ser reiterativa, se presentará a consideración del Comité Institucional de Coordinación de Control Interno, para que adopte las decisiones pertinentes.

5. Acompañar y asesorar metodológicamente a los procesos, en la administración y gestión integral de riesgos, en coordinación con la segunda línea de defensa.

6. Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.

7. Comunicar al Comité de Coordinación de Control Interno posibles cambios evidenciados en la evaluación del riesgo, detectados durante las auditorías.

8. Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

Tabla. Roles y responsabilidades para la administración del riesgo por procesos

Línea de defensa	Responsable	Responsabilidad frente al riesgo
Línea estratégica	Consejo de gobierno Comité de coordinación de control interno Comité institucional de gestión y desempeño	Esta línea al ser una instancia decisoria dentro del sistema de Control Interno, su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la Línea Estratégica: • Fortalecimiento del Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para las reuniones. • Evaluación de la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica. • Definición de líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. • Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. • Evaluación de la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar)
		Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.
Primera línea de defensa	Líderes de procesos y sus equipos de trabajo	Esta línea está bajo la responsabilidad, principalmente, de los líderes de procesos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la organización); su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de

		riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol". Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 1ª Línea: • El conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. • La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.
Segunda línea de defensa	Secretaría de Planeación	• El seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. • La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. • La coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa.
	• Secretaría de las TIC o Jefe de la Oficina Asesora de Informática, Secretaría de Hacienda • Jefe Oficina Jurídica	• Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los
	•Comité de Contratación •Comité de conciliaciones	

		controles seleccionados para el tratamiento de los riesgos identificados. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del Comité de Coordinación de Control Interno. • Actualizar, según se requiera, los escenarios de riesgo bajo su responsabilidad
		Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 2ª Línea son: • Aseguramiento de que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. • Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
		• Realizar el seguimiento al mapa de riesgos de su proceso. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • La (El) Jefe de Oficina Jurídica tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Trabajo coordinado con las oficinas de control interno en el fortalecimiento del Sistema de Control Interno. • Establecimiento de los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora).

Tercera línea de defensa	Oficina de Control Interno	Esta línea está bajo la responsabilidad de la (el) Jefe de control interno; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 3ª Línea: • A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Secretaría de Planeación. • Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. • Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. • Informar los hallazgos y proporcionar recomendaciones de forma independiente. • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Recomendar mejoras a la política de operación para la administración del riesgo.

13. MONITOREO

Los monitoreos le corresponden a: la línea estratégica, primera y segunda línea de defensa y se desarrollarán de la siguiente manera:

Línea estratégica: el comité de Coordinación de Control Interno realizará monitoreo cada semestre, para verificar el cumplimiento de la política de administración de riesgos.

Estos se reportarán a través de los (formatos, herramientas y/o instrumentos que los responsables determinen)

Primera línea de defensa: Realiza monitoreo bimestral a las acciones tendientes a controlar y gestionar los riesgos y enviará a la Secretaría de Planeación los resultados de esos monitoreos quince días antes de terminarse el bimestre. Estos se reportarán a través de los (formatos, herramientas y/o instrumentos que los responsables determinen)

Segunda línea de defensa: Realizará monitoreo bimestral a través de los informes que los líderes de procesos remitan, asegurando que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. Estos se reportarán a través de los (formatos, herramientas y/o instrumentos que los responsables determinen)

Para los riesgos del proceso de contratación, la primera línea de defensa debe realizar un monitoreo constante dado que las circunstancias cambian rápidamente y los riesgos no son estáticos. La matriz y el plan de tratamiento deben ser revisadas constantemente y, si es necesario, hacer ajustes al plan de tratamiento de acuerdo con las circunstancias. Sumado a lo anterior, la primera línea de defensa debe monitorear los riesgos y revisar la efectividad y el desempeño de las herramientas implementadas para su gestión. Para lo cual, debe: (i) asignar responsables; (ii) fijar fechas de inicio y terminación de las actividades requeridas; (iii) señalar la forma de seguimiento (encuestas, muestreos aleatorios de calidad, u otros); (iv) definir la periodicidad de revisión; y (v) documentar las actividades de monitoreo.

14. SEGUIMIENTO

El seguimiento le corresponde a la tercera línea de defensa, la oficina de control interno quien provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos

de manera que contribuya al logro en el cumplimiento de los objetivos institucionales y de proceso, así como frente a los riesgos de corrupción.

Nota: Los ajustes al mapa de riesgos es permanente, por lo cual se debe hacer envío a la Secretaría de Planeación del mapa actualizado, para que sea publicado, máximo 10 días posteriores al recibo de este.

Nota: Para los riesgos identificados en el proceso de contratación la responsabilidad de la segunda línea de defensa se dirige a la oficina de contratación.

Si algún riesgo se llegara a materializar y esto es detectado por el líder del proceso se deben seguir los siguientes pasos:

1. Informar o reportar al Representante de la Alta Dirección del MIPG.
2. Según corresponda, realizar la denuncia ante el ente de control respectivo.
3. Iniciar con las acciones correctivas necesarias.
4. Realizar el análisis de causas y determinar acciones de mejora.
5. Análisis y actualización del mapa de riesgos.

Nota: Si se llega a materializar algún riesgo del proceso de contratación se debe informar a la oficina de contratación y a la oficina de control interno.

Además de la evaluación de riesgos, la oficina de Control Interno valorará el estado de la implementación, la efectividad de las medidas de administración, el diseño de los controles, junto con el nivel final de exposición al riesgo.

Si la oficina de Control Interno en los seguimientos establecidos evidencia que un riesgo de corrupción se materializó, debe seguir los siguientes pasos:

1. Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la

investigación de los hechos.

2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.

3. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.

Los procesos de contratación de bienes y servicios y el de atención al ciudadano, deberán tener en cuenta los criterios establecidos por el Programa Presidencial para la moralización, eficiencia, transparencia y lucha contra la corrupción, en lo referente con lo establecido en la Ley 1474 de 2011.

15. FUENTES DE CONSULTA

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. Departamento Administrativo de la Función Pública (DAFP). Diciembre, 2020. En: Biblioteca virtual EVA. Función Pública. Enlace: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499 Accessed: 2021-08-17.

- Guía de Auditoría para Entidades Públicas. Enlace: https://www.funcionpublica.gov.co/documents/418537/506911/Manual+T%C3%A9cnico+del+Modelo+Est%C3%A1ndar+de+Control+Interno+para+el+Estado+Colombiano+MECI+2014/065a3838-cc9f-4eeb-a308-21b2a7a040bd Accessed: 2021-08-17.

- Modelo de gestión de cumplimiento centrado en la transparencia y en la prevención de la corrupción incluido el soborno (GC-TCS) Enlace: https://www.icontec.org/wp-content/uploads/2019/11/Modelo-de-Gestio%CC%81n-GC-TCS-4.pdf Accessed: 2021-08-17.

CONTROL DE CAMBIOS

VERSIÓN	FECHA VERSION	DESCRIPCIÓN DE CAMBIOS
1.0	2019	Establece la Política Distrital de Administración de Riesgos de acuerdo con la guía de administración de riesgos versión 2018- DAFP.
2.0	2021	Se revisó y actualizó la política teniendo en cuenta los lineamientos de la nueva metodología de administración de riesgos – DAFP (calificación de probabilidad e impacto, explicación al nivel de aceptación, responsabilidades frente a la gestión y materialización de riesgos).
Revisó		**Aprobó**
NOMBRE: Juan David Franco Peñaloza CARGO: Secretario de planeación		NOMBRE: Comité de coordinación de control interno CARGO: No aplica
Formuló: Secretaría de planeación, equipo MIPG		