Alcaldía Mayor de
Cartagena de Indias

POLITICA DE ADMINISTRACION DEL RIESGO

ENERO DE 2025

VERSIÓN 4.0

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

CONTROL DE CAMBIOS

VERSIÓN	AÑO	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).
3.0	**2023**	• Se mantiene estructura conceptual para la administración del riesgo. • Se incluye la definición del contexto estratégico. • Se incluye capítulo específico sobre riesgo fiscal, que se complementa con el Anexo denominado catalogo indicativo de puntos de riesgo fiscal para facilitar el análisis en el marco del modelo de operación por Procesos
4.0	**2025**	• Se ajustan los siguientes apartes: • Objetivo de la Política • Alcance de la Política • Responsabilidades de las líneas de defensa. • Metodología para el Análisis de Riesgos y Valoración de Controles, precisando conceptos asociados a éstos • Se modifica capítulo de Riesgos de Seguridad de la información para incluir metodología y responsabilidades de una manera más clara

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

1. INTRODUCCIÓN

La gestión de riesgos es una herramienta clave para que las entidades públicas puedan alcanzar sus metas de manera eficiente y transparente. Disponer de procesos claros y efectivos que identifiquen, prevengan y mitiguen riesgos, no solo fortalece la confianza ciudadana, sino que también impulsa una cultura de mejora continua y buen gobierno, más aún, en un contexto donde la administración de los recursos públicos enfrenta grandes retos.

Esta política nace con el objetivo de establecer los lineamientos para la implementación de la política de riesgos en la Alcaldía Mayor de Cartagena de Indias, siguiendo las metodologías definidas y establecidas en las versiones 4 y 6 de la ***Guía para la Administración de Riesgos y Diseño de Controles en Entidades Públicas***, y en el ***Documento Técnico del Programa de Transparencia y Ética Pública***. Aquí se establecen recomendaciones prácticas para anticiparse a eventos que puedan afectar la gestión o dar lugar a situaciones de corrupción, buscando siempre la protección de los recursos y la generación de resultados que beneficien a la ciudadanía.

En el marco del **Modelo Integrado de Planeación y Gestión – MIPG –**, esta política no solo presenta herramientas técnicas, sino que también promueve la construcción de una cultura organizacional basada en el autocontrol, la transparencia y la rendición de cuentas. Somos conscientes que gestionar riesgos no es tarea de unos pocos, sino un compromiso que involucra a todos los servidores públicos, independientemente de su rol dentro de la entidad.

Partiendo de la premisa que 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; esta Política contribuye a que la entidad consolide su Sistema de Control Interno y a generar una cultura de Autocontrol y autoevaluación al interior de esta.

Por último, el verdadero valor de esta política no radica solo en los procedimientos, sino en la voluntad de quienes la implementan. Cada acción tomada para identificar, evaluar y controlar riesgos contribuirá a una administración más eficiente, ética y orientada al servicio de los cartageneros. Con ella, esperamos que la Alcaldía Distrital de Cartagena de Indias siga avanzando hacia un gobierno más fuerte, transparente y preparado para enfrentar los desafíos del presente y del futuro.

2. OBJETIVO

Establecer lineamientos y procedimientos en la Alcaldía Mayor de Cartagena de Indias para la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos institucionales incluyendo aquellos asociados a planes, programas y proyectos, que permita autogestionarlos impactando el cumplimiento de los objetivos estratégicos y operativos y promoviendo una cultura organizacional de autocontrol y mejora continua, en concordancia con el Modelo Estándar de Control Interno (MECI) y el Modelo Integrado de Planeación y Gestión (MIPG).

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

3. ALCANCE

Esta política aplica a todos los procesos establecidos en el modelo de operación por procesos de la Alcaldía Mayor de Cartagena de Indias, reflejándose en las acciones ejecutadas durante el ejercicio de la gestión de los funcionarios, servidores y contratistas, a través del cumplimiento de los procedimientos y metodologías establecidos en cada una de las tipologías de riesgos, abarcando los procesos, planes y proyectos definidos en el modelo de operación de la entidad. El enfoque en riesgos debe considerarse en todas las actividades claves de los procesos, planes, programas y proyectos que se desarrollen en las diferentes dependencias y entidades del Distrito y comprende desde la identificación de Riesgos hasta la aplicación de acciones de mejora o tratamiento de riesgos a partir del autocontrol y la evaluación independiente.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

4. BENEFICIOS DE LA GESTIÓN DE RIESGOS

La gestión de los riesgos institucionales da acceso a los siguientes beneficios inherentes:

- **Alinea el riesgo y la estrategia:** En su evaluación de alternativas estratégicas, la dirección considera los riesgos priorizados por la entidad, estableciendo los objetivos correspondientes y desarrollando mecanismos para gestionar las oportunidades o amenazas asociadas.

- **Mejora las decisiones de respuesta a los riesgos:** La gestión de riesgos institucionales proporciona rigor para identificar las posibles oportunidades o amenazas que hacen parte del que hacer institucional y seleccionar entre las posibles alternativas de respuesta a las amenazas o a las oportunidades, la más viable y efectiva para alcanzar los resultados esperados.

- **Reduce los resultados no deseados y las pérdidas operativas:** La gestión de los riesgos mejora la capacidad de la Entidad para identificar las amenazas o vulnerabilidades que pueden afectar su gestión y establecer respuestas, reduciendo aquellos resultados no deseados y las pérdidas asociadas.

- **Identifica y gestiona la diversidad de riesgos para toda la entidad:** La entidad se enfrenta a riesgos que inciden de manera negativa o positiva en el desempeño de sus procesos y en el logro de los resultados planificados; la gestión de riesgos facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos.

- **Provee respuestas integradas a múltiples riesgos:** La ejecución de los procesos conllevan riesgos inherentes, para lo cual la gestión de los riesgos favorece la elaboración de soluciones integradas para administrarlos, bajo la premisa de optimizar los recursos disponibles y garantizar la coherencia en las respuestas institucionales, en el momento de abordar las posibles vulnerabilidades o amenazas, así como las oportunidades identificadas.

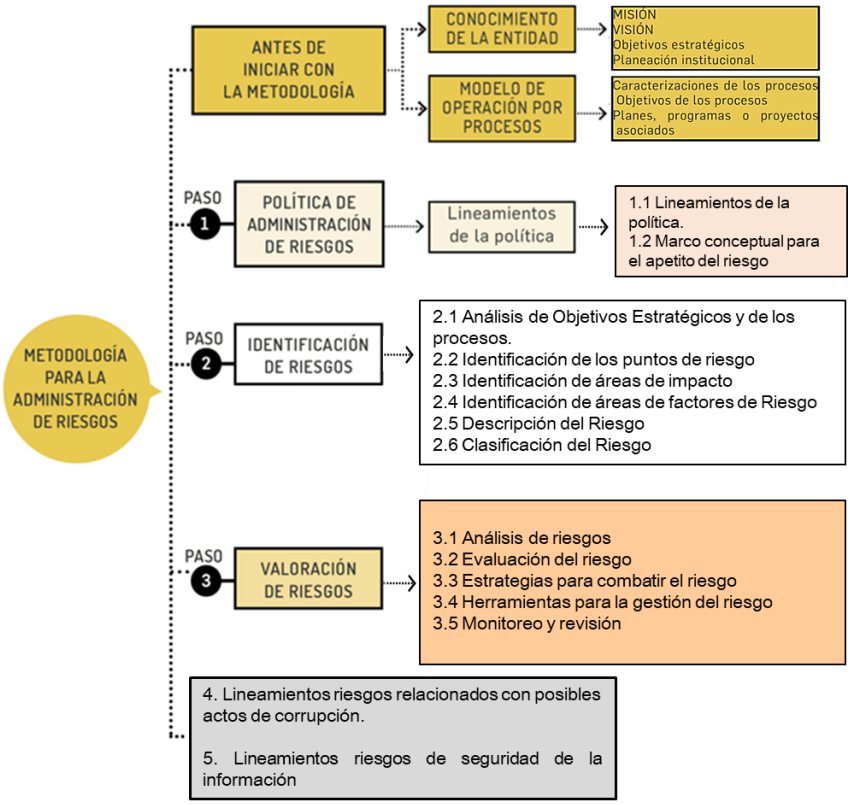
- **Permite aprovechar las oportunidades:** mediante la consideración de una amplia gama de potenciales eventos, la Entidad está en posición de identificar y aprovechar las oportunidades de modo proactivo, a fin de potencializar los efectos deseables.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

5. METODOLOGÍA 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 V6 emitida en noviembre de 2022 por el Departamento Administrativo de la Función Pública, 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:



Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6 / Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

6. GLOSARIO

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.
Activo de Información: Cualquier recurso que contenga, procese o soporte la información de la organización. Esto incluye datos, hardware, software, personas y procesos. (ISO/IEC 27001:2013)
Administración de riesgos: 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000).
Análisis de riesgo: Uso sistemático de la información disponible para valorar los riesgos en función de las causas o agentes que los generan, las consecuencias generadas por un incidente y/o evento, su severidad y la posibilidad de ocurrencia de este, con el fin de estimar la zona de riesgo inicial (riesgo inherente).
Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
Causa: Medios, circunstancias, situaciones o agentes generadores del riesgo. Algunas fuentes de riesgos son: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.
Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
CGDI: Comité de Gestión y Desempeño Institucional.
CICCI: Comité Institucional de Coordinación de Control Interno.
Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Consecuencia: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento
Control: Cualquier medida que adopte la entidad para gestionar los riesgos y proporcionar una seguridad razonable de alcanzar los objetivos y metas establecidos
Contingencia: Posible evento futuro, condición o eventualidad.
Continuidad: Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
Crisis (Emergencia): Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Disponibilidad: Propiedad que garantiza que los usuarios autorizados puedan acceder a la información y los sistemas asociados cuando sea necesario (ISO/IEC 27001:2013)
Evaluación del riesgo: Determinación de las prioridades de gestión del riesgo, mediante la comparación del nivel de riesgo hallado (riesgo inherente) y la evaluación de las medidas de control existentes. Es una etapa que busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).
Factores de Riesgo: Son las fuentes generadoras de riesgos.
Fraude: Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.
Gestión del riesgo: Es el conjunto de "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Contempla las etapas de política de administración del riesgo, construcción del mapa de riesgos, comunicación y consulta, monitoreo y revisión y seguimiento.
Gestor de Riesgos: Persona o rol responsable de liderar el proceso de gestión de riesgos dentro de la organización (NIST SP 800-39)
Incidente de Seguridad de la Información: Evento que compromete la confidencialidad, integridad o disponibilidad de la información o los sistemas que la procesan (ISO/IEC 27035:2011)
Integridad: Propiedad de la información que garantiza que los datos sean exactos, completos y estén protegidos contra modificaciones no autorizadas (ISO/IEC 27001:2013)
Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Mapas de riesgo: Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.
MECI: Modelo Estándar de Control Interno
MIPG: Modelo Integrado de Planeación y Gestión
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.
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 d e l orden nacional, departamental y municipal**.**
Plan de tratamiento de riesgos: Se define como las decisiones de tratamiento de los riesgos y las actividades de control para su mitigación, a través de la aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de ocurrencia de los riesgos, sus consecuencias o ambas.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Política de Administración del Riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o Administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.
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.
Restablecimiento: Capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.
Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. En el contexto de la seguridad de la información, se define como la posibilidad de que una amenaza explote una vulnerabilidad, causando un impacto negativo.
Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Riesgo Fiscal: Riesgo de pérdidas sobre bienes y recursos públicos; su administración se basa en el catálogo de puntos de riesgo fiscal de la Guía DAFP.
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.
Riesgos Operativos: Posibilidad de incurrir en pérdidas por errores, fallas o deficiencias en el Talento Humano, Procesos, Tecnología. Infraestructura y Eventos Externos
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.
Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

7. MARCO LEGAL Y NORMATIVO.

- **Decreto 1122 de 2024,** Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011 y se establece el Programa de Transparencia y Ética Pública - PTEP
- **Ley 2195 de 2022,** por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción.
- **Ley 1581 de 2012 y Decreto 1377 de 2013**: Protección de datos personales.
- **Ley 1273 de 2009**: Define delitos informáticos y protege la integridad de los datos.
- **Ley 1712 de 2014**: Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Circular Básica Jurídica de la Superintendencia Financiera (Capítulo XXII): Gestión de riesgos asociados a la seguridad de la información en entidades financieras.
- **Circular 15 de 2017** de la Superintendencia de Industria y Comercio sobre seguridad de la información.
- **Decreto 620 de 2020:** Política de seguridad digital Fortalece la política de seguridad digital para entidades públicas, incluyendo la gestión de riesgos de seguridad de la información.
- **Circular Conjunta 100-01 de 2021**: Emite directrices para la implementación de seguridad digital en entidades públicas.
- **MIPG**: Gestión de riesgos en el sector público.
- **ISO/IEC 27001 e ISO/IEC 31000**: Estándares internacionales de gestión de seguridad de la información y riesgos.
- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP)**.
- **Modelo Nacional de Gestión de Riesgos de Seguridad de la Información**.
- **Guía de Orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Entidades Territoriales y Sector Público**.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

8. PRINCIPIOS RECTORES

- **Proactividad**: La Alcaldía priorizará la prevención y detección temprana de riesgos.

- **Responsabilidad Compartida**: La administración de riesgos es una tarea compartida en toda la organización, bajo el esquema de líneas de defensa.

- **Mejora Continua**: Implementación de controles y acciones correctivas adaptadas al contexto y evolución de los riesgos.

- **Estructura y Responsabilidades según el Esquema de Líneas de Defensa:**

Línea de Defensa	Responsabilidad
Línea Estratégica *(Consejo de gobierno – Comité Institucional de Control Interno – Comité Institucional de Gestión y Desempeño)*	▪ Analizar los riesgos y amenazas que puedan afectar los planes estratégicos ▪ Aprobar los lineamientos que permitan cumplir con la administración de Riesgos en el Distrito de Cartagena (Política de Riesgos) ▪ Analizar los resultados de los informes de seguimiento y establecer medidas a aplicar de acuerdo con los resultados obtenidos ▪ Fortalecer el Comité Institucional de Coordinación de Control Interno.
Primera Línea de Defensa *(Unidades operativas y líderes de proceso)*	▪ Identificación y gestión de riesgos en su área de responsabilidad. ▪ Documentación y comunicación de los riesgos y controles implementados. ▪ Participación en capacitaciones periódicas en gestión de riesgos.
Segunda Línea de Defensa *(Áreas de gestión de riesgos)*	▪ Supervisión de la efectividad de la gestión de riesgos en la primera línea. ▪ Asesoría a las unidades en la implementación de controles específicos para riesgos gestión, de corrupción, fiscales y de seguridad de la información. ▪ Monitoreo a la gestión de riesgos a través de monitoreo a la implementación de los controles y los planes de acción aplicados sobre los riesgos residuales ▪ Elaboración desarrollo de informes de seguimiento y monitoreo a la gestión del riesgo.
Tercera Línea de Defensa *(Oficina Asesora de Control Interno)*	▪ Evaluación independiente de la efectividad de la gestión de riesgos. ▪ Identificación de áreas de mejora mediante auditorías basadas en niveles de riesgo.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

9. ROLES Y RESPONSABILIDADES

En virtud de la integración de la gestión del riesgo con la estrategia de la entidad, medida a través de la plataforma estratégica, resulta importante precisar que la formulación e implementación de los objetivos estratégicos tiene lugar en la toma de decisiones cotidiana en cada uno de los procesos.

Bajo este entendido, el desarrollo de la gestión integral del riesgo opera en los diferentes niveles de la organización, por lo que cada entidad, de acuerdo con su esquema de operación por procesos, tendrá insumos esenciales para iniciar con la aplicación de la metodología propuesta para la administración del riesgo, de acuerdo con el esquema de líneas de defensa incorporado en el marco del Modelo Integrado de Planeación y Gestión que permite identificar y asignar los roles y responsabilidades a los funcionarios y a los diferentes órganos de dirección de la Alcaldía Mayor de Cartagena de Indias.

Así las cosas, los roles y responsabilidades en la gestión integral del riesgo para cada línea de defensa se detalla a continuación:

Línea Estratégica: Conformada por Alta dirección en el marco del Comité Institucional de Coordinación de Control Interno, *a quienes corresponde:*

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

5. 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.

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

7. Brindar orientación sobre la administración de los riesgos de la Entidad.

8. Evaluar los planes de tratamiento establecidos para cada uno de los riesgos

materializados, minimizando la posibilidad de que el evento se repita.

Primera Línea de Defensa: **Le corresponde a Gerentes públicos y Líderes de procesos en la Alcaldía Mayor de Cartagena**, quienes tendrán que:

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 los lineamientos para la administración de riesgos vigentes.

3. Realizar, con el apoyo de su equipo de trabajo, la administración de los riesgos identificados. Así mismo, analizar, valorar, 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, de acuerdo con las metodologías establecidas y demás directrices frente al tema, comunicando a la Secretaría de Planeación los cambios que considere pertinentes.

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

7. Evaluar periódicamente la eficacia de los controles definidos para gestionar los riesgos identificados y actualizarlos cada vez que se presenten cambios en el proceso donde operan.

8. 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.

9. Reportar los planes de tratamiento establecidos para cada uno de los riesgos materializados, incluyendo las actividades para prevenir su repetición, así como las causas que dieron origen a la materialización de dichos eventos.

Segunda Línea de Defensa: En concordancia con la Guía para la administración de riesgos y diseño de controles en entidades públicas Versión 6, esta línea de defensa está conformada por **servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección**.

En la Alcaldía mayor de Cartagena de Indias, en la segunda línea de defensa están incluidos la Secretaría de Planeación, la Oficina Asesora Informática, la Secretaría de Hacienda, la Oficina Asesora Jurídica, Servidores con cargos de nivel Directivo o asesor, responsables de monitoreo y seguimiento a la implementación de controles y quienes realizan labores de supervisión sobre los temas referentes a riesgos en la entidad y rinden cuentas ante la Alta Dirección.

Secretaría de Planeación:

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

2. Adelantar el monitoreo del mapa de riesgos, verificando el cumplimiento en la implementación de los controles y acciones establecidas para la mitigación de riesgos, y visibilizando todas aquellas situaciones que dificulten o impidan la administración de los riesgos, en concordancia con la cultura del autocontrol y autoevaluación 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 de la administración de riesgos, a través de las herramientas dispuestas para tal fin.

5. Consolidar y publicar los mapas de riesgos por procesos.

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 de Informática

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

2. Implementar la metodología para la identificación y gestión de riesgos de seguridad de la información, de acuerdo con la política de seguridad digital, lo lineamientos impartidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones, en el marco de la tercera dimensión del Modelo Integrado de Planeación y Gestión.

3. Acompañar y asesorar metodológicamente a los procesos del Distrito, en la administración y gestión de riesgos de seguridad de la información.

4. Adelantar el monitoreo del mapa de riesgos de seguridad de la información, verificando el cumplimiento en la implementación de los controles y acciones establecidas para su mitigación, 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.

Secretaria de Hacienda

Implementar la metodología para la identificación y gestión de riesgos de acuerdo con los lineamientos establecidos en política de gestión presupuestal y eficiencia del gasto público.

La Secretaría de Hacienda Distrital de Cartagena, en su rol de segunda línea de defensa, tiene como responsabilidades y funciones supervisar, monitorear y apoyar la implementación de las estrategias de gestión de riesgos fiscales, con el objetivo de garantizar la sostenibilidad fiscal y el uso eficiente de los recursos públicos, además:

1. Implementar metodología para la gestión de los riesgos fiscales, que permita establecer criterios para identificar, evaluar los riesgos y establecer controles para situaciones que puedan afectar la estabilidad financiera del distrito.

2. Establecer procedimientos y normativas que aseguren una adecuada administración de los riesgos fiscales en el Distrito.

3. Evaluar y monitorear los riesgos fiscales derivados de situaciones que puedan generar resultados no deseados o desviaciones a los objetivos institucionales.

4. Proporcionar asesoría técnica a las dependencias del Distrito con relación a los riesgos fiscales que pueden presentarse en sus respectivas áreas de trabajo, con el fin de implementar acciones correctivas de manera oportuna.

5. Promover la capacitación y sensibilización de los servidores públicos sobre la importancia de gestionar los riesgos fiscales.

6. Diseñar mecanismos que permitan prever y prevenir situaciones que puedan poner en peligro la liquidez del distrito, como el no cumplimiento de metas de ingresos o un gasto público desmesurado.

Oficina Asesora Jurídica

La Oficina Asesora Jurídica, en su rol de segunda línea de defensa, tiene la responsabilidad de garantizar que se implementen adecuadamente mecanismos de control y mitigación de riesgos desde un enfoque legal, institucional y normativo.

1. Asesorar legalmente al Alcalde, los Secretarios de Despacho y otras entidades distritales en materia de gestión de riesgos asociados a la gestión jurídica.
2. Garantizar que las acciones del Distrito en términos de prevención y mitigación de riesgos estén alineadas con la legalidad.
3. Participar en la adopción de políticas y normativas internas relacionados con la gestión de riesgos.
4. Asesorar en la capacitación y sensibilización de los servidores públicos distritales sobre los riesgos legales inherentes a sus funciones y sobre la importancia de la gestión de riesgos.
5. Evaluar los riesgos jurídicos que pueden surgir de proyectos distritales, como obras públicas o iniciativas de desarrollo, asegurándose de que estén bien estructurados desde el punto de vista legal.

Desde el punto de vista contractual, la Oficina Asesora Jurídica Distrital tendrá las siguientes responsabilidades:

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.

Tercera Línea de Defensa: **Le corresponde a la Oficina de Control Interno**, la cual debe:

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 observaciones y hallazgos, 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.

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

Tabla 1. Roles y responsabilidades para la administración del riesgo por procesos

LÍNEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Línea estratégica	Consejo de Gobierno	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:
		• Fortalecer el Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para las reuniones.
	Comité de Coordinación de Control Interno	• Evaluar la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica.
		• Definir las líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa.
	Comité Institucional de Gestión y Desempeño	• Analizar la Gestión del Riesgo y aplicar las mejoras, considerando los cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes.
		• Evaluar la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar) teniendo en cuenta los principios de igualdad, transparencia, el mérito, el compromiso y la imparcialidad.
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".
		• Considerar los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 1ª Línea:
		• Conoce y apropiar las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo.
		• Identificar riesgos y establecer 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	• Adoptar a través de la Política de Riesgos Institucionales la metodología para la identificación y gestión de riesgos, de acuerdo con la normatividad y los lineamientos establecidos, para cada una de las tipologías, a excepción de aquellas que requieren un desarrollo metodológico particular por su naturaleza, tales como: los ambientales, los fiscales, los de seguridad y salud en el trabajo y los de seguridad de la información.
		• Adelantar el monitoreo del mapa de riesgos, verificando el cumplimiento en la implementación de los controles y acciones establecidas para la mitigación de riesgos, y visibilizando todas aquellas situaciones que dificulten o impidan la administración de los riesgos, en concordancia con la cultura del autocontrol y autoevaluación al interior de la Entidad.
		• 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	• Formular lineamientos que orienten a los procesos para que se desarrolle de manera eficaz, eficiente y efectiva la gestión de riesgos de seguridad de la información.
		• Determinar e implementar la metodología para la identificación y gestión de riesgos de seguridad de la información, de acuerdo con la política de seguridad digital, lo lineamientos impartidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones, en el marco de la tercera dimensión del Modelo Integrado de Planeación y Gestión.

		• Acompañar y asesorar metodológicamente a los procesos del Distrito, en la administración y gestión de riesgos de seguridad de la información.
		• Adelantar el monitoreo del mapa de riesgos de seguridad de la información, verificando el cumplimiento en la implementación de los controles y acciones establecidas para su mitigación, 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.
	Secretaria de Hacienda	• Implementar metodología para la gestión de los riesgos fiscales, que permita establecer criterios para identificar, evaluar los riesgos y establecer controles para situaciones que puedan afectar la estabilidad financiera del distrito.
		• Establecer procedimientos y normativas que aseguren una adecuada administración de los riesgos fiscales en el Distrito.
		• Evaluar y monitorear los riesgos fiscales derivados de situaciones que puedan generar resultados no deseados o desviaciones a los objetivos institucionales.
		• Proporcionar asesoría técnica a las dependencias del Distrito con relación a los riesgos fiscales que pueden presentarse en sus respectivas áreas de trabajo, con el fin de implementar acciones correctivas de manera oportuna.
		• Promover la capacitación y sensibilización de los servidores públicos sobre la importancia de gestionar los riesgos fiscales.
	Oficina Asesora Jurídica	• Asesorar legalmente al Alcalde, los Secretarios de Despacho y otras entidades distritales en materia de gestión de riesgos.
		• Brindar orientación sobre la interpretación y aplicación de normativas, regulaciones y leyes relacionadas con la gestión de riesgos
		• Garantizar que las acciones del Distrito en términos de prevención y mitigación de riesgos estén alineadas con la legalidad.
		• Participar en la adopción de políticas y normativas internas relacionados con la gestión de riesgos.
		• Asesorar en la capacitación y sensibilización de los servidores públicos distritales sobre los riesgos legales inherentes a sus funciones y sobre la importancia de la gestión de riesgos.
Segunda línea de defensa	Oficina Asesora Jurídica (Contractual)	• 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.
		• 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.
		• 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.
		• 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.

Tercera Línea de Defensa	Oficina Asesora 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. • Asesorar metodológicamente a los procesos, en la administración y gestión integral de riesgos, en coordinación con la segunda línea de defensa. • 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.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

10. DEFINICIÓN DEL CONTEXTO ESTRATÉGICO

Con el fin de identificar los factores externos e internos que inciden en el desempeño de los procesos y en el logro de las metas y objetivos establecidos en la planeación estratégica, se debe identificar el contexto externo, interno y del proceso.

FACTORES INTERNOS Y EXTERNOS DE RIESGO	
CONTEXTO EXTERNO	**CONTEXTO INTERNO**
Se determina las características o aspectos esenciales del entorno en el cual opera la entidad, retoma los siguientes factores:	Se determina las características del ambiente en el cual la organización busca alcanzar sus objetivos, se analizan aspectos como:
Económicos: Disponibilidad de recursos financieros, liquidez, mercados financieros, desempleo, competencia.	Financieros: Presupuesto funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
Político: cambios de gobierno, legislación, políticas públicas, regulación	Personal: Competencia y disponibilidad de personal, seguridad y salud laboral.
Medioambientales: Condiciones ambientales, residuos, energía, agua, catástrofes naturales, desarrollo sostenible	Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento, interacción, transversalidad, responsables, lineamientos internos definidos, registros.
Seguridad y Salud en el Trabajo: Condiciones de Seguridad y salud en el trabajo externas, emergencias, eventos catastróficos, residuos peligrosos.	Seguridad y Salud en el Trabajo: Condiciones de Salud, condiciones de trabajo, presupuesto, recursos, infraestructura, comunicación, responsabilidades.
Sociales y Culturales: Demografía, responsabilidad social, orden público.	Estructura organizacional: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, interrupciones, tecnología emergente, gobierno en línea.	Tecnología: avances tecnología, acceso al sistema de información externo, gobierno en línea.
Comunicación Externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad	Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Tabla 2. Características por Tipo Contexto

CONTEXTO DEL PROCESO
Diseño del proceso: Claridad en la descripción del alcance y objeto del proceso
Interrelación con otros procesos: Claridad en la descripción del alcance y objetivo del Proceso
Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad
Procedimientos asociados: pertinencia en los procedimientos que desarrolla el proceso
Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso
Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

11. METODOLOGÍA

11.1. RIESGOS DE GESTIÓN

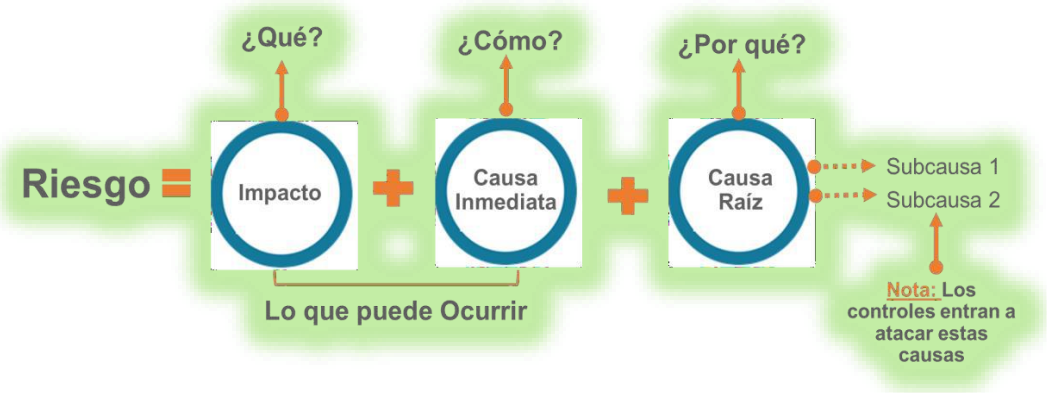
La metodología para la Administración del Riesgo en la Alcaldía Mayor de Cartagena de Indias se define a partir de los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión vigente, teniendo en cuenta las etapas de identificación, valoración y seguimiento.

11.1.1. Identificación y Descripción de Riesgos

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, teniendo en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Para la Alcaldía Mayor de Cartagena de Indias se identificarán los riesgos a los objetivos estratégicos y a todos los procesos de la entidad, como mínimo un riesgo por proceso u objetivo con el respectivo análisis e identificación de los factores de riesgo como son: (Procesos, Talento Humano, Tecnología, Infraestructura, eventos externos) y las áreas de impacto como la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse el riesgo.

Con respecto a la descripción del riesgo se tendrá en cuenta la siguiente estructura:



- **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:** Causa principal o básica, corresponde 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 puede existir más de una causa o sub-causas que pueden ser analizadas.

  Cada uno de los elementos de la etapa de identificación se describe e incorporan en la herramienta de matriz del riesgo de la entidad. Ver anexo A.

11.1.2. Valoración de Riesgos

La valoración de los riesgos consiste en establecer la probabilidad de ocurrencia, su posible impacto para determinar el nivel de severidad o criticidad del riesgo. Esa valoración se realiza a través de la aplicación de dos elementos o acciones: el Análisis del Riesgo y la Evaluación de los controles aplicados al mismo.

11.1.2.1. Análisis de Riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto. Este análisis nos permite identificar el RIESGO INHERENTE.

Esta etapa tiene como objetivo establecer la probabilidad de ocurrencia del riesgo, es decir, la exposición que tiene la entidad frente al riesgo y el impacto o consecuencias que se pueden generar, con el fin de determinar la zona de severidad del riesgo inherente, así mismo, se diseñan y analiza la efectividad de los controles.

Es importante tener en cuenta que, el análisis de la severidad del riesgo inicial o inherente tiene en cuenta dos factores no excluyentes, es decir, se analizan de manera complementaría. Por lo tanto, su severidad debe ser determinada tanto por la probabilidad de ocurrencia, como por el impacto que generaría su materialización, así las cosas, aunque la probabilidad sea baja, si su impacto es alto, su severidad estará enmarcada en una zona de calor que requiere la implementación de control necesarias.

11.1.2.1.1. Determinación de la Probabilidad

La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, es decir el número de veces que se ejecuta la acción.

Dado que el riesgo Inherente se define como aquel propio de la actividad o al que se está expuesto con la realización misma de la actividad, su probabilidad de ocurrencia estará medido por el número de veces que esta se realiza en el período a considerar.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Lo anterior, permite determinar con total claridad la frecuencia con la cual se lleva a cabo una actividad y no los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de la entidad.

Teniendo en cuenta lo explicado anteriormente sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 3 se establecen los criterios y rangos para definir el nivel de probabilidad, los cuales son adoptados de la tabla sugerida por el Departamento Administrativo de la Función Pública[1].

Tabla 3: Criterios para definir el nivel de Probabilidad.

	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%

[1] Tabla 3 Criterios para definir el nivel de probabilidad – Guía para la Administración del riesgo y el Diseño de Controles en Entidades Públicas (Versión 6).

11.1.2.1.2. Determinación del Impacto

Con respecto al impacto se tendrá en cuenta las áreas identificadas en la descripción del riesgo y se analizará frente a los criterios y rangos definidos en la tabla 4 para definir el nivel de impacto, los cuales son adoptados de la tabla sugerida por el Departamento Administrativo de la Función Pública presentada a continuación:

Tabla 4. Criterios para definir el nivel de Impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

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

Tabla 4 Criterios para definir el nivel de Impacto – Guía para la Administración del riesgo y el Diseño de Controles en Entidades Públicas (Versión 6).

Tal como se muestra en la tabla anterior, la afectación económica está medida en términos de la cantidad de salarios mínimos legales mensuales vigentes (SMLMV) en que se ve afectada la entidad por la materialización del riesgo o la ocurrencia del hecho no deseado mientras la afectación reputacional mide el daño o deterioro a l imagen de la entidad.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto.

11.1.2.2. Evaluación del Riesgo

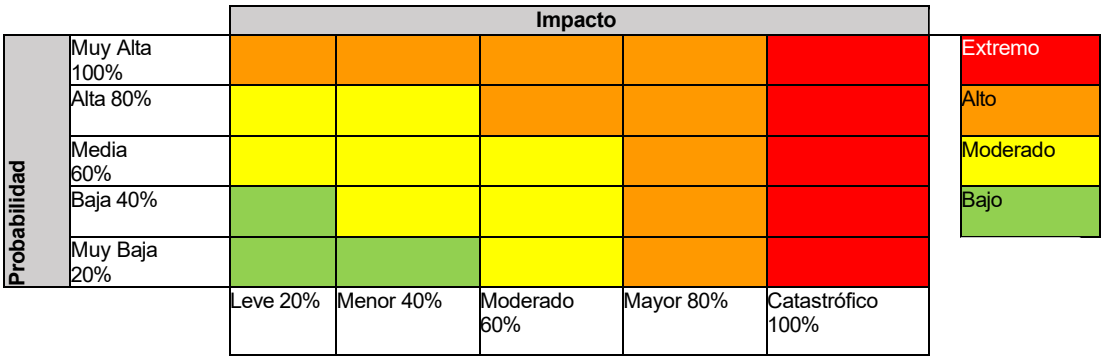
11.1.2.2.1. Análisis Preliminar (Riesgo Inherente)

En esta etapa, una vez analizado el riesgo identificado y descrito para determinar la probabilidad y el impacto, se debe realizar el análisis de esta probabilidad e impacto identificado para determinar el nivel de severidad del riesgo inherente, a través de la combinación de probabilidad e impacto en el mapa de calor.

Para la determinación del nivel de severidad del riesgo inherente, se definen cuatro (4) zonas de severidad como se observa en la matriz de calor que se presenta a continuación. (Ver figura 1).

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Figura: 1



11.1.2.3. Valoración de los Controles

Un control se define como la medida que permite reducir o mitigar el riesgo, por lo tanto, es necesario identificar controles a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto. Adicional los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la Descripción del Control:

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

Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se identificará el sistema que realiza la actividad.

Acción: Se determina mediante verbos, en los cuales se identifica la acción a realizar como parte del control. Se debe expresar de forma explícita el propósito del control y como se ejecutará para controlar la materialización de efecto no deseado.

Complemento: Corresponde a los detalles que permitan identificar claramente el objeto del control. Es decir que, este debe incluir periodicidad para su ejecución, observaciones o desviaciones resultantes de la ejecución y evidencia de la ejecución.

De igual manera, se tendrá una tipología de controles a través del ciclo de procesos que permitirá saber cuándo se debe activar el control. Los controles pueden ser preventivos, detectivos o correctivos.

- **Control preventivo:** Acción y/o mecanismo ejecutado antes que se realice la actividad originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.
- **Control detectivo:** Acción y/o mecanismo ejecutado que permite detectar el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo. Estos controles detectan el riesgo, pero genera reprocesos.
- **Control correctivo:** Acción que se ejecutan después de que se materializa el riesgo y en la mayoría de las ocasiones permiten reducir el impacto de dicho riesgo.

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

- **Control manual:** Controles que son ejecutados por una persona.
- **Control automático:** Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.

La Alcaldía Mayor de Cartagena de Indias, define los controles teniendo en cuenta la estructura para su descripción, la tipología y la manera como se implementa, se debe tener en cuenta que los controles de tipo preventivo y detectivo mitigan la probabilidad de ocurrencia y los controles detectivos el impacto del riesgo, por lo tanto, es necesario revisar qué tipo de controles se deben definir para mitigar los riesgos identificados en la entidad.

Es de aclarar, que según el tipo de control (preventivo, detectivo o correctivo) y su implementación (automático o manual) tienen un peso porcentual que se debe determinar para realizar la correspondiente valoración del riesgo inherente y servirá para realizar el respectivo desplazamiento en el mapa de calor y conocer el riesgo residual.

A continuación, se establecen los criterios para el diseño del control, es de aclarar que mínimo se deben garantizar la tipología y la implementación del control para conocer la eficiencia de este y los otros atributos se determinan bajo el criterio del líder del proceso de manera informativa.

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%

	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control, lo cual llevará a determinar el riesgo inherente una vez aplicados los controles y establecido su nivel de efectividad.

Si bien es cierto que los atributos informativos no desplazan el riesgo en la matriz de calor, estos se hacen necesarios para establecer los elementos del control y asegurar que su descripción contenga todos los elementos necesarios para su evaluación, asi mismo, permite garantizar la identificacion adecuada de los soportes y evidencias del control.

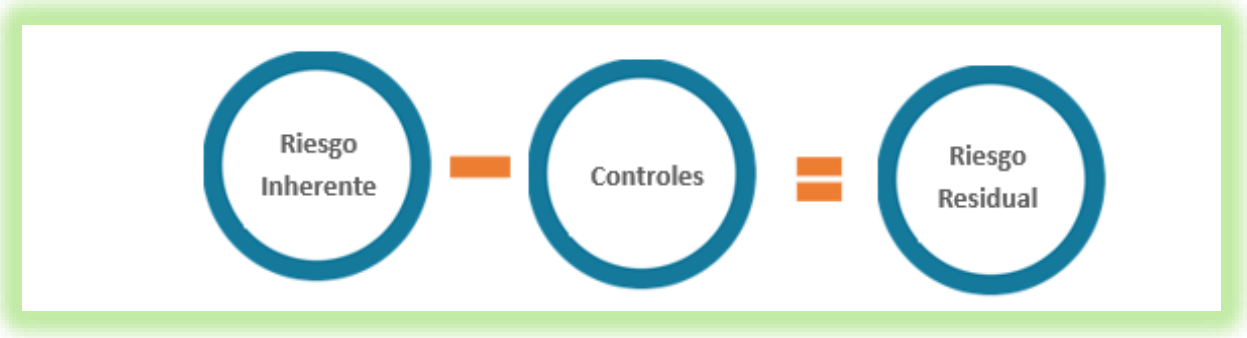
La grafica No 2 ilustra los movimientos que pueden presentarse a partir de la aplicación de los controles. Estos movimientos pueden darse en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Figura: 2

					Controles Correctivos → Atacan Impacto				
					Impacto				
Controles Preventivos y Detectivos	↓	Atacan Probabilidad	Probabilidad	Muy Alta 100%					
				Alta 80%					
				Media 60%					
				Baja 40%					
				Muy Baja 20%					
					Lev e 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

11.1.2.3.1. Nivel de Riesgo (Riesgo Residual)

De acuerdo con lo anterior, el resultado de aplicar la efectividad de los controles al riesgo inherente nos determina el riesgo residual.



Dependiendo del nivel de severidad en que se ubique el riesgo residual, la Arcadia Mayor de Cartagena de Indias, priorizará la atención en aquellos riesgos residuales que todavía se encuentren en un nivel de severidad alto y extremo y se define su tratamiento y posibles acciones a seguir.

11.1.2.4. Tratamiento del Riesgo

El tratamiento a un determinado nivel de riesgo se analiza frente al riesgo residual, sin embargo, para procesos nuevos se realizará sobre el riesgo inherente.

Las decisiones frente al tratamiento del riesgo se determinarán conforme las opciones que se presentan en la tabla 5.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Tabla 5. Criterios para tratamiento de riesgos de gestión

Zona Severidad Residual	Estrategia de tratamiento / Periodicidad de Seguimiento
BAJO	La decisión es ACEPTAR el riesgo y determinar ASUMIR el mismo conociendo los efectos de su posible materialización.
	El seguimiento a sus controles es SEMESTRAL a través de informes de seguimiento.
MODERADO	La decisión es ACEPTAR el riesgo y determinar ASUMIR el mismo conociendo los efectos de su posible materialización.
	No obstante, a decisión del líder del proceso se podrá tomar la decisión de REDUCIR el riesgo mediante la MITIGACIÓN a través de un plan de acción o la TRANSFERENCIA del impacto económico a través de seguros o pólizas.
	En cualquier caso, el seguimiento es de manera TRIMESTRAL a través de la presentación de informes.
ALTO	La decisión es REDUCIR el riesgo mediante la MITIGACIÓN a través de un plan de acción o la TRANSFERENCIA del impacto económico a través de seguros o pólizas y el seguimiento es de manera MENSUAL a través de informes de seguimiento.
	La decisión es REDUCIR el riesgo mediante la MITIGACIÓN a través de un plan de acción o la TRANSFERENCIA del impacto económico a través de seguros o pólizas.
	Igualmente, a decisión del líder del proceso se podrá tomar la decisión de EVITAR el riesgo NO asumiendo ejecutar la actividad que genera este riesgo, siempre y cuando normativamente sea posible.
EXTREMO	En este caso, esta opción deberá ser analizada y aprobada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno.
	En cualquier caso, el seguimiento es de manera MENSUAL a través de la presentación de informes.

En caso de establecer un plan de acción para mitigar el riesgo, como herramienta de planificación que permite la gestión y control de tareas para reducir al máximo el nivel del riesgo es necesario que el líder del proceso determine las actividades, responsables, fechas de implementación y seguimiento.

Para mayor claridad en el Anexo A de la presente política se establece el desarrollo metodológico para la identificación, valoración y tratamiento de riesgos, así mismo, en el anexo B se establece el mapa de riesgos con un ejemplo aplicado que permite entender el desarrollo de la metodología y su paso a paso.

11.2. RIESGOS DE CORRUPCIÓN

En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción. Es importante recordar que el desarrollo de este componente se articula con los demás establecidos para el desarrollo

del plan, ya que se trata de una acción integral en la lucha contra la corrupción.

Respecto de la gestión de riesgos de corrupción, como un componente de la gestión integral del riesgo en la entidad, la Alcaldía Mayor de Cartagena de Indias ha decidido adoptar los lineamientos y parámetros impartidos por la Secretaría de Transparencia a través del Numeral 4 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 5), conforme se detalla en cada una de las etapas que se describen a continuación.

11.2.1. Identificación y Descripción De Riesgos

En materia de riesgos asociados a posibles actos de corrupción, respecto de su identificación se deben considerar los siguientes aspectos:

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

Ahora bien, respecto de la descripción específica de cada riesgo y conforme lo señala el Numeral 2.2. de la mencionada Guía, en la Alcaldía Mayor de Cartagena de Indias se debe dar respuesta a cada una de las preguntas clave que se presentan a continuación, las cuales conducirán a la descripción del riesgo de corrupción observando la siguiente estructura, la cual se sugiere en la mencionada Guía.

Preguntas Clave

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

Ejemplo

Preguntas Clave			
¿Qué puede suceder?	**¿Cómo puede suceder?**	**¿Cuándo puede suceder?**	**¿Qué consecuencias tendría su materialización?**
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros		Cuando se adelanta el proceso contractual	Celebrar un contrato.

Matriz de Definición/Descripción del Riesgo de Corrupción				
Descripción del Riesgo	**Acción u Omisión**	**Uso del Poder**	**Desviar la Gestión de lo Público**	**Beneficio Privado**

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

11.2.2. VALORACIÓN DE RIESGOS

11.2.2.1. Análisis de Riesgos

11.2.2.1.1. *Determinación de la Probabilidad*

La Alcaldía Mayor de Cartagena de Indias, acorde con lo señalado por la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 5), ha determinado adoptar los lineamientos descritos en el Numeral 4, por lo tanto, para determinar la probabilidad de los riesgos de corrupción se deben utilizar los rangos de la Tabla 3 presentada en el Numeral 8.1.2.1.1. de la presente Política de Administración de Riesgos.

Criterios para calificar la probabilidad

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

(Fuente DAFP)

Tabla: 3: Criterios para definir el nivel de probabilidad

	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%

11.2.2.1.2. *Determinación del Impacto*

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción la Alcaldía Mayor de Cartagena de Indias aplicará los lineamientos impartidos en el Numeral 4. de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 5), por lo tanto, para determinar el impacto de los riesgos de corrupción se deberán contestar las preguntas descritas en la tabla 6.

Tabla 6. Preguntas de impacto

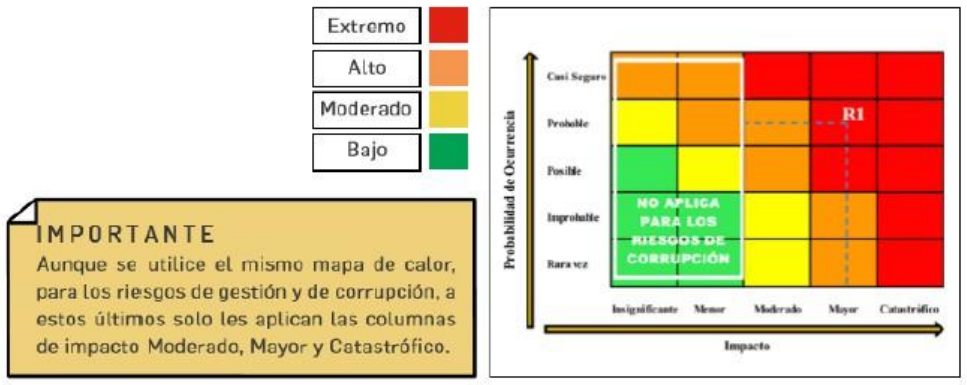
N°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA …	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de los servicios?		
8	¿Dar lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar perdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		

11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humana?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto MODERADO.			
Responder afirmativamente de SEIS a ONCE preguntas(s) genera un impacto ALTO.			
Responder afirmativamente de DOCE a DIECINUEVE preguntas(s) genera un impacto CATASTROFICO.			

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

Respecto de la determinación del impacto es importante precisar que, dada la naturaleza de los riesgos de corrupción, y conforme lo señala la Guía en su numeral 4, frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles de severidad:

i) Moderado
ii) Mayor, y
iii) Catastrófico



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

11.2.2.2. Evaluación del Riesgo

11.2.2.2.1. Análisis Preliminar (Riesgo Inherente)

En esta etapa, una vez analizado el riesgo identificado y descrito para determinar la probabilidad y el impacto, se debe realizar el análisis de esta probabilidad e impacto identificado para determinar el **nivel de severidad del riesgo inherente**, a través de la combinación de probabilidad e impacto en el mapa de calor.

Para la determinación del **nivel de severidad del riesgo inherente**, se definen tres (3) zonas de severidad como se observa en la matriz de calor que se presenta a continuación (Ver figura 3), acorde con lo señalado en el Numeral 8.1.2.2.1 de la presente política respecto de los niveles de impacto válidos para los riesgos de corrupción.

Figura: 3

		Impacto				
Probabilidad	Muy Alta 100%	Zonas NO Validas Para Riesgos De Corrupción				
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy Baja 20%					
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado

11.2.2.2.2. Valoración de los Controles

Conforme se señala en el Numeral 4 de la Guía, para la valoración de los controles para la gestión de riesgos de corrupción, se aplicarán los lineamientos y pesos porcentuales mencionados en el Numeral 8.1.2.2.2. de la presente Política.

11.2.2.2.3. Nivel de Riesgo (Riesgo Residual)

De acuerdo con lo anterior, el resultado de aplicar la efectividad de los controles al riesgo inherente nos determina el riesgo residual

Dependiendo del nivel de severidad en que se ubique el riesgo residual, la Alcaldía Mayor de Cartagena de indias priorizará la atención en aquellos riesgos residuales que todavía se encuentren en un nivel de severidad alto y extremo y se define su tratamiento y posibles acciones a seguir.

No obstante, por tratarse de riesgos de corrupción se debe considerar que en ninguna circunstancia es admitido la determinación de un nivel de impacto residual

en los niveles menor y leve, es decir, se debe considerar el mapa de calor definido en el Numeral 8.1.2.2.3

11.2.2.3. Tratamiento del Riesgo

El tratamiento a un determinado nivel de riesgo se analiza frente al riesgo residual, sin embargo, para procesos nuevos se realizará sobre el riesgo inherente.

Las decisiones frente al tratamiento del riesgo se determinarán conforme las opciones que se presentan en la tabla 7.

Tabla 7. Criterios para tratamiento de riesgos de corrupción

Zona Severidad Residual	Estrategia de Tratamiento / Periodicidad de Seguimiento
MODERADO	La decisión es **REDUCIR** el riesgo mediante la **MITIGACIÓN** a través de un plan de acción o la **TRANSFERENCIA** del impacto económico a través de seguros o pólizas y el seguimiento es de manera **MENSUAL** a través de informes.
ALTO	La decisión es **REDUCIR** el riesgo mediante la **MITIGACIÓN** a través de un plan de acción o la **TRANSFERENCIA** del impacto económico a través de seguros o pólizas.
	Igualmente, a decisión del líder del proceso se podrá tomar la decisión de **EVITAR** el riesgo **NO** asumiendo ejecutar la actividad que genera este riesgo, siempre y cuando normativamente sea posible.
EXTREMO	En este caso, esta opción deberá ser analizada y aprobada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno.
	En cualquier caso, el seguimiento es de manera **MENSUAL** a través de informes.

Conforme a lo presentado anteriormente es preciso señalar que, por tratarse de un riesgo de corrupción, **en ninguna circunstancia un riesgo de corrupción puede ser aceptado**.

11.3. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

11.3.1. Identificación de activos de información

De acuerdo con las directrices del Archivo General de la Nación, que establecen la metodología adecuada para el tratamiento de los "tipos de información y documentos físicos y electrónicos, así como los sistemas, medios y controles asociados a la gestión", la identificación y clasificación de los activos de información deben articularse de manera integral.

En este sentido, los propietarios y custodios de la información producida en cada área son responsables de identificar, clasificar y valorar los activos de información siguiendo las directrices establecidas. Esto incluye apoyarse en una compilación de activos como: Información; Software (programas informáticos); Hardware (equipos de cómputo y periféricos); Servicios; Personas (con sus calificaciones, habilidades y experiencia); e Intangibles (como reputación e imagen).

La identificación de los activos debe realizarse con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

En el contexto de la seguridad de la información, los activos incluyen, entre otros, los siguientes elementos:

- **Hardware** (equipos de cómputo, servidores y dispositivos tecnológicos).
- **Software** (sistemas operativos, aplicaciones y licencias).
- **Aplicaciones de la entidad** (desarrollos propios o adquiridos).
- **Servicios web** y plataformas digitales.
- **Redes** (infraestructura de conectividad).
- **Información digital** (datos y documentos electrónicos).
- **Personal** (empleados y contratistas).
- **Ubicación** (infraestructura física y centros de datos).
- **Estructura organizacional** (roles, procesos y relaciones internas).
- **Tecnologías de la Información (TI)** y **Tecnologías de la Operación (TO)** (sistemas de control y sensores) utilizadas por la entidad para su funcionamiento.

Es fundamental llevar a cabo la identificación de los activos de información y documentar un inventario detallado de los mismos. Para este propósito, la Alcaldía de Cartagena cuenta con el instructivo GTIGPS01-I006, titulado "Instructivo para la Identificación y Clasificación de los Activos de Información".

La identificación y valoración de los activos debe ser realizada por la Primera Línea de Defensa — representada por los Líderes de Proceso—, en cada uno de los procesos donde se aplica la gestión del riesgo de seguridad de la información. Este proceso debe

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

estar debidamente orientado por el responsable de seguridad digital o el responsable de seguridad de la información de la entidad.

A continuación, se detallan los pasos para la identificación y valoración de los activos de información:

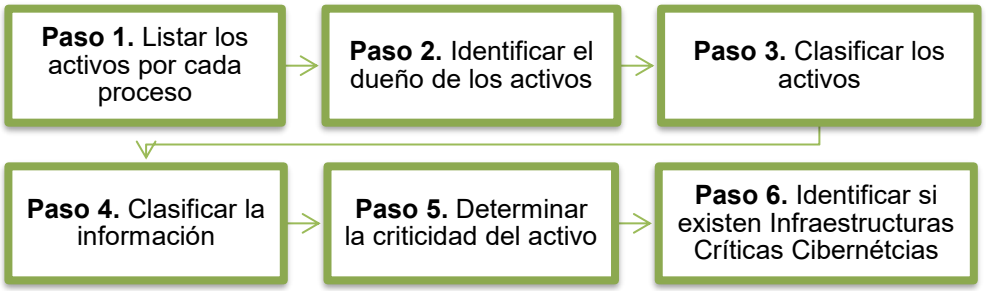


Figura 1. Pasos para la identificación y valoración de activos.
Fuente: MinTIC

La Alcaldía Distrital de Cartagena utiliza el formato GTIGPS01-F007 "Formato de Inventario y Clasificación de Activos de Información" para realizar el levantamiento e inventario de los activos, siguiendo los seis (6) pasos previamente descritos. Esta información se convierte en el insumo principal del formato GTIGPS01-F001, denominado "Mapa de Riesgos OAI", donde se registran los activos seleccionados del formato GTIGPS01-F007, los cuales serán objeto de la gestión de riesgos.

Tabla. Ejemplo identificación activos del proceso

PROCESO	ACTIVO	DESCRIPCIÓN	DUEÑO DEL ACTIVO	TIPO DE ACTIVO	LEY 1712 DE 2014	LEY 1581 DE 2012	CRITICIDAD RESPECTO A SU CONFIDENCIALIDAD	CRITICIDAD RESPECTO A SU INTEGRIDAD	CRITICIDAD RESPECTO A SU DISPONIBILIDAD	NIVEL DE CRITICIDAD
Gestión nómina	Base de datos de nómina	Base de datos con información de nómina de la entidad	DATH	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión nómina	Aplicativo de nómina	Servidor web que contiene el front office de la entidad	DATH	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Tesorería	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

11.3.2.Identificación y Descripción de Riesgos

Como base para la identificación de los riesgos de seguridad de la información se debe tomar el índice de activos de información del proceso previamente elaborado.

Posteriormente se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

1. Pérdida de la confidencialidad
2. Pérdida de la integridad

3. Pérdida de la disponibilidad

Seguidamente, para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, la Alcaldía Mayor de Cartagena de Indias se basa en las tablas que establece la Guía para la Administración de Riesgos y Diseño de controles en Entidades Públicas en su Anexo de Instructivo de Riesgos de Seguridad Digital. Entre ellas, la Tabla No. 8 muestra el resumen de Amenazas y Vulnerabilidades de seguridad digital más comunes.

Tabla 8. Tabla de Amenazas y Vulnerabilidades más Comunes

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección física	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
Red	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes	Uso no autorizado del equipo

	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Ausencia del personal	Incumplimiento en la disponibilidad
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
Personal	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
Lugar	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Hurto de medios o documentos
	Ubicación en área susceptible de inundación	Destrucción de equipos o medios
	Red energética inestable	Falla en equipo de telecomunicaciones
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
Organización	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso

	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Fuente: MinTIC

11.3.2.1.1. *Determinación de la Probabilidad*

La Alcaldía Mayor de Cartagena de Indias, acorde con lo señalado por la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 5), ha determinado adoptar los lineamientos descritos en el Numeral 5.2., por lo tanto, para determinar la probabilidad de los riesgos de seguridad digital se deben utilizar los rangos de la Tabla 3 presentada en el Numeral 11.1.2.1.1 de la presente Política de Administración de Riesgos.

11.3.2.1.2. *Determinación del Impacto*

La Alcaldía Mayor de Cartagena de indias, acorde con lo señalado por la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 5), ha determinado adoptar los lineamientos descritos en el Numeral 5.2., por lo tanto, para determinar el impacto de los riesgos de seguridad digital se deben utilizar los rangos de la Tabla 4 presentada en el Numeral 11.1.2.1.2. de la presente Política de Administración de Riesgos.

11.3.3. Evaluación del Riesgo

11.3.3.1.1. *Análisis Preliminar (Riesgo Inherente)*

En esta etapa, una vez analizado el riesgo identificado y descrito para determinar la probabilidad y el impacto, se debe realizar el análisis de esta probabilidad e impacto identificado para determinar el nivel de severidad del riesgo inherente, a través de la combinación de probabilidad e impacto en el mapa de calor.

Para la determinación del nivel de severidad del riesgo inherente, se definen cuatro (4) zonas de severidad acorde con el mapa de calor adoptado en el Numeral 11.1.2.2.1.

11.3.3.1.2. *Valoración de los Controles*

Conforme se señala en el Numeral 5.4. de la Guía, los riesgos de seguridad de la información se controlan empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013 que presenta la Guía, los cuales se encuentran en el anexo 4. "*Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas*", siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

Así las cosas, la Alcaldía Mayor de Cartagena de Indias decide adoptar los lineamientos para el diseño y valoración de controles incorporados en los anexos señalados anteriormente.

11.3.3.1.3. *Instructivo para la Identificación y Valoración de Riesgos de Seguridad Digital.*

En el marco de la implementación de la presente política de Riesgos, la Oficina Asesora de Informática emitirá instructivo estandarizado que detalle el paso a paso y las herramientas a considerar para la gestión de riesgos de seguridad digital, el cual será la guía aplicable al Distrito de Cartagena para este fin.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

12. LINEAMIENTOS PARA EL ANÁLISIS DE RIESGO FISCAL

12.1. CONTROL FISCAL INTERNO Y PREVENCIÓN DEL RIESGO FISCAL

La construcción de este capítulo tiene como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. Para tener claro el ámbito normativo y jurídico, es necesario precisar que sus bases están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, los cuales fueron modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

A partir de lo anterior, el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave como:

- **Control fiscal Multinivel**: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

- **Control fiscal Interno (CFI):** Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

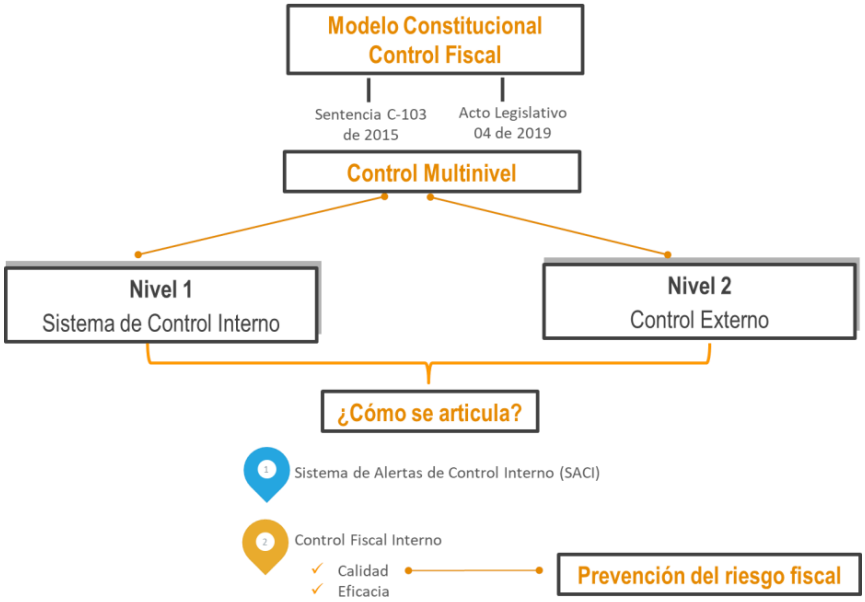
En el nuevo modelo constitucional el control externo adquiere un enfoque preventivo y a su vez el control interno potencia el enfoque preventivo, partiendo de la premisa de que el Sistema de Control Interno es fundamental para conjugar el logro de resultados, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labor es de cobro, entre otros), a través de la prevención de responsabilidades.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

La figura 4 muestra este despliegue y sus elementos de articulación que sustentan el desarrollo del presente capítulo.

- **Figura 4: Articulación modelo constitucional control fiscal y sistema de control interno**

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.



A continuación, se presenta el paso a paso de la gestión del riesgo fiscal (Identificación, análisis y valoración), que debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso.

La metodología que se propone es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite, mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos.

Como parte integral de la metodología propuesta se pone a disposición, como insumo de referencia, un Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas (ver anexo),el cual ha sido construido como resultado del análisis de precedentes (aproximadamente 130 fallos con responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República) y debe ser utilizado como marco de referencia para la identificación y valoración de riesgos fiscales, siempre atendiendo las particularidades, naturaleza, complejidad, recursos, usuarios o grupos de valor, portafolio de productos y servicios, sector en el cual se desenvuelva (contexto), así como otras condiciones específicas de cada entidad.

En consecuencia, cada entidad deberá analizar si existen, de acuerdo con su contexto y particularidades puntos de riesgos y circunstancias inmediatas diferentes a los identificados en dicho catalogo y tenerlas en cuenta en la identificación de sus riesgos fiscales.

12.2. DEFINICIÓN Y ELEMENTOS DEL RIESGO FISCAL

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

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

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

12.3. METODOLOGÍA Y PASO A PASO PARA EL LEVANTAMIENTO DEL MAPA DE RIESGOS FISCALES

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, que es fundamental para el resultado de la gestión de cada entidad y para la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual,

supervisores, responsables de labores de cobro, entre otros).

Paso 1: identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Ahora bien, para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de gestión fiscal en las que potencialmente se genera riesgo fiscal) y circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal). Para este taller, puede usar las siguientes preguntas orientadoras:

Tabla 11. Preguntas: orientadoras para puntos riesgo fiscal y causas inmediatas

Preguntas y respuestas para la identificación
¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Preguntas y respuestas para la identificación
Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces. En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? **Nota:** Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.
¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo1), son aplicables a la entidad?

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Identificación de áreas de impacto

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

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.
Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.

- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo uno de conceptos básicos).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (I) bienes públicos; (II) recursos públicos o (III) intereses patrimoniales de naturaleza pública (consultar definiciones en el capítulo uno de conceptos básicos).

Identificación de la causa raíz o potencial hecho generador

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

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal.

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial

hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño - efecto- (Contraloría General de la República, 2021)[3]

Ejemplo:

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

¿Cuál es el daño? El daño fiscal corresponde al monto pagado por concepto de intereses moratorios

¿Cuál es el hecho generador? La omisión de pagó oportuno del canon de arrendamiento.

Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

Descripción del Riesgo Fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta:

- Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.

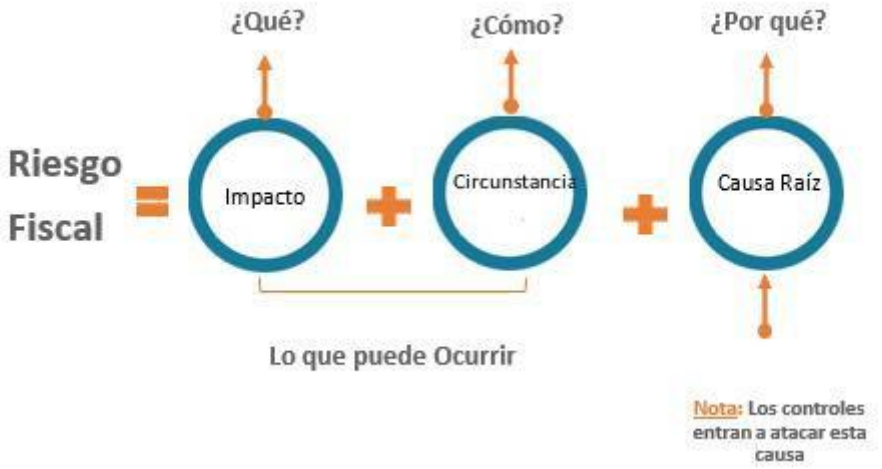
- **Impacto**: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

- **Circunstancia inmediata**: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica - causa raíz- para que se presente el riesgo.

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

- **Causa Raíz**: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:



Ejemplo:

Proceso: Gestión de Recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre bienes públicos	Por pérdida, extravío o hurto de bienes muebles de la entidad.	A causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública.

Tabla 12. Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Paso 2: Valoración del riesgo fiscal Evaluación de riesgos

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

Probabilidad

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

Teniendo esto de presente, para definir el nivel de probabilidad, se ha de tener en cuenta la siguiente tabla definida en el numeral 8.1 de la presente política:

	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 de3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de24 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%

Nota: Es necesario mencionar, que las frecuencias pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que las frecuencias en cada nivel pueden ser adaptadas a las necesidades y complejidad de cada entidad.

Impacto

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

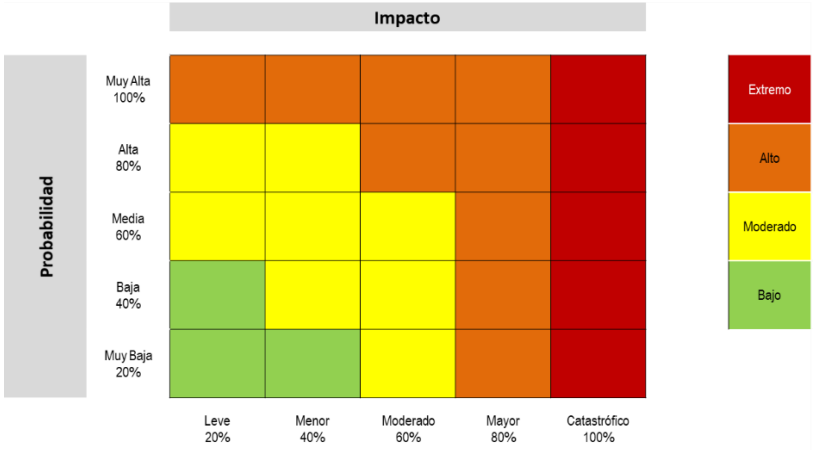
Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la siguiente tabla definida en el numeral 8.1 de la presente política:

Nota: Es necesario mencionar, que los niveles en la afectación económica pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que los rangos en cada nivel pueden ser adaptados a las necesidades y complejidad de cada entidad.

Determinación del nivel de riesgo inherente

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o

impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad, para lo cual se aplica la matriz definida en el numeral 8.1.2.2.1 de la presente política:



Nota: Es necesario mencionar, que esta matriz de severidad está diseñada de acuerdo con estándares internacionales que permiten tener trazabilidad en los desplazamientos en cada zona, por lo que se recomienda no modificarla.

Ejemplo (continuación):

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad

varían en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.
Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año	100%

La actividad se Realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es **media.**

Para determinar el impacto es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de $2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico

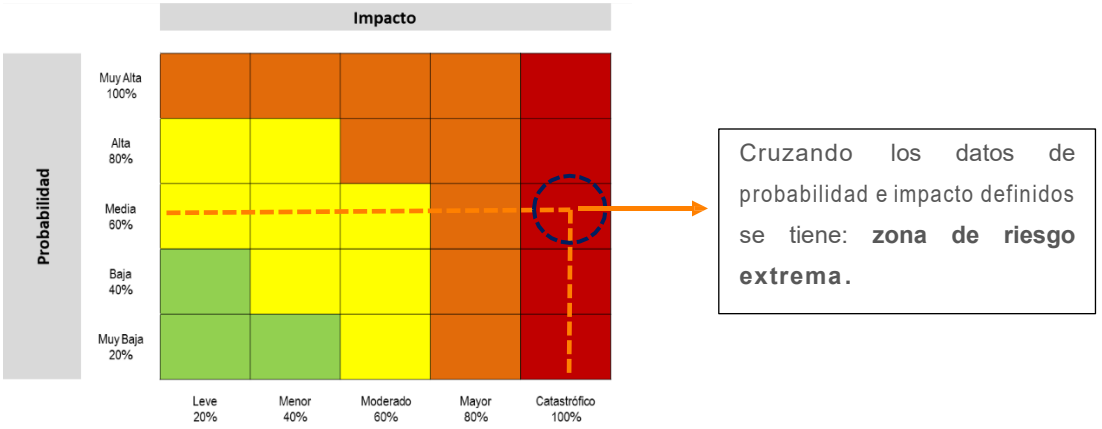
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

La afectación económica se calcula en más de 500SMLMV, el impacto del riesgo es **catastrófico.**

Probabilidad inherente = media 60%, **Impacto inherente:** catastrófico 100%

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un

nivel de riesgo extremo.



Paso 3. Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.
Tipologías de controles:

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

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

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

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Se aplican los lineamientos para la redacción del control establecidos en el numeral 8.1.2.2.1 y tabla definida en el numeral 8.1.2.1.1 de la presente política.

Ejemplo (continuación):

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad Inherente: Media 60% **Impacto Inherente:** Catastrófico 100% **Zona de riesgo:** Extrema

Controles Identificados:

- Control 1 Preventivo: El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.

- Control 2 Detectivo: El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.

- Control 3 Correctivo: El director administrativo verifica la vigencia y actualización de la póliza de acuerdo con los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador

Aplicando la tabla de valoración de controles tenemos:

Control 1	Criterios de efectividad			Peso
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 1 =40%			

El Centro, Cartagena de Indias- Cra. 2 #36-86 alcalde@cartagena.gov.co Tel: (605)6411370

Control 2	Criterios de efectividad			Peso
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Tipo	Preventivo		
		Detectivo	x	15%
		Correctivo		
	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 2 = 30%			

Control 3	Criterios de efectividad			Peso
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo con los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	x	10%
	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 3 = 25%			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y su respectiva valoración, a fin de determinar el riesgo residual.

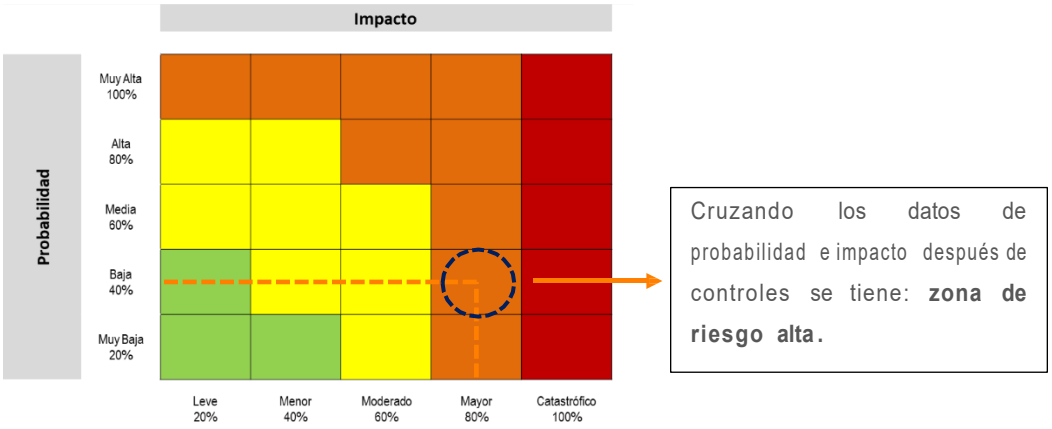
Nivel de riesgo (riesgo residual):

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Para mayor claridad a continuación, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión de cumplimiento del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% =24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 Detectivo	30%	36%* 30% =10.8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2%			
	Impacto Inherente	100%	Valoración control correctivo	25%	100%* 25% =25% 100% - 25% = 75%
	Impacto Residual	75%			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor, a continuación, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y cálculo final:



La anterior información puede trasladarse a la matriz mapa de riesgo que hace parte de los anexos desarrollados para la presente guía.

12.4. SEGUIMIENTO

- Los riesgos operativos se validan cada vez que sea necesario, atendiendo la metodología vigente.

- La periodicidad de seguimiento a los controles y plan de acción de mitigación de

cada riesgo está definida de acuerdo con la zona de severidad donde se encuentre cada riesgo. Así las cosas, entre más severos, más estricto será el seguimiento al control, para garantizar su ejecución.

- El líder de cada proceso analizara los resultados del seguimiento y puede determinar establecer un plan de mejoramiento cuando se presente cualquier desviación del objetivo o resultado esperado y socializar al interior de su dependencia las acciones a seguir.

- El líder de cada proceso comunica, revisa y actualiza, con el acompañamiento de la Secretaría de Planeación el mapa de riesgo ante cualquier modificación en sus controles o plan de acción.

12.5. 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 Institucional de Coordinación de Control Interno realizará monitoreo cada semestre, para verificar el cumplimiento de la política de administración de riesgos.

Primera línea de defensa:

Realizará el monitoreo de los riesgos identificados teniendo en cuenta la periodicidad asignada para la ejecución de los controles y enviará reporte trimestralmente, (5) cinco días hábiles posteriores al cierre de cada trimestre los resultados de esos monitoreos a la Secretaría de Planeación.

Para el reporte al monitoreo, deberá suministrarse:

- Informe de análisis de la primera línea de defensa que incluya acciones de mejora establecidas según los resultados,
- La medición al seguimiento en el período realizado,
- Las evidencias a la aplicación de controles y la gestión de riesgos
- Y se utilizarán los formatos, herramientas y/o instrumentos estandarizados, adoptados y socializados para su seguimiento de acuerdo con los lineamientos de la Secretaría de Planeación

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.

Segunda línea de defensa:

Realizará monitoreo trimestral a partir 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, se ejerzan por el responsable y apropiadamente y funcionen como se pretende.

Estos se reportarán a través de los formatos, herramientas y/o instrumentos estandarizados, adoptados y socializados para su seguimiento de acuerdo con los lineamientos que la Secretaría de Planeación establezca para tal fin.

12.6. HERRAMIENTA PARA LA GESTIÓN DEL RIESGO

La Alcaldía Mayor de Cartagena de Indias determina que el mapa de riesgos es la herramienta para la identificación, valoración, tratamiento y seguimiento a los riesgos, por lo tanto, toda la información que requiere la entidad para el seguimiento y análisis es provista por esta herramienta, para lo cual la Secretaria de Planeación asesora y socializa la metodología descrita, hace seguimiento al cumplimiento de los lineamientos establecidos en esta política y revisa de acuerdo a la periodicidad definida para el nivel de severidad de los riesgos y su tratamiento el cumplimento de las acciones.

Igualmente se establece como herramienta para el acompañamiento los informes de primera y segunda línea generados de manera trimestral y en los cuales se consignará el análisis a los resultados tanto de la gestión como del seguimiento a la administración de riesgos, según corresponda.

Revisó	Aprobó
NOMBRE: CAMILO REY SABOGAL **CARGO:** Secretario de Planeación **Firma**	**NOMBRE:** Comité Institucional de Coordinación de Control Interno. **CARGO**: No Aplica **Acta No. 01** **Fecha: enero 29-2025**

Actualizó: Equipo MIPG /Secretaría de Planeación