TABLA DE CONTENIDO

1. INTRODUCCIÓN 5
2. OBJETIVO 6
3. ALCANCE 6
4. NORMATIVIDAD 6
5. MARCO CONCEPTUAL 6
6. ROLES Y RESPONSABILIDADES 9
7. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS 11
8. RUTA DE IMPLEMENTACIÓN 12
8.1. Metodología para la Gestión Integral del Riesgo 12
8.2. Determinación del Nivel de madurez 14
8.3. Metodología para la Gestión Integral del Riesgo 14
8.4. Apetito, Tolerancia y Capacidad del Riesgo. 15
8.5. Identificación de riesgos. 16
8.5.1. Clasificación del Riesgo por Factor 20
8.6. Identificación de áreas de impacto 20
8.7. Identificación de áreas de factores de riesgo 21
8.8. Estructura de la descripción del Riesgo 22
8.8.1. Valoración del Riesgo 23
8.8.2. Análisis del Riesgo Inherente 23
8.8.3. Zonas de severidad 24
8.9. Diseño, Análisis y Valoración de Controles 25
8.9.1. Diseño de controles 25
8.10. Aplicación de controles y Riesgo residual 28
8.11. Tratamiento del Riesgo 30
8.12. Consolidación en el mapa de riesgos. 30
9. TIPOLOGÍAS DE RIESGO 31
9.1. Riesgos de Gestión. 31
9.2. Riesgos de Seguridad de la Información. 32

9.2.1. Identificación de los activos de seguridad de la información. 32
9.2.2. Identificación de Riesgos de Seguridad de la información. 33
9.2.3. Consolidación en el Mapa de Riesgos 36
9.3. Riesgos Fiscales 36
9.3.1. Identificación de áreas de factores de riesgo 37
9.3.2. Identificación del Riesgo 37
9.3.3. Identificación de Puntos de Riesgo Fiscales y Causa Inmediata 37
9.3.4. Identificación de áreas de impacto 38
9.3.5. Identificar el efecto económico 39
9.3.6. Identificación de la causa raíz o potencial hecho generador 39
9.3.7. Descripción del Riesgo Fiscal 39
9.4. Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP 41
9.4.1. Integridad pública 42
9.4.2. Amenazas para la integridad pública. 43
9.4.2.1. Soborno 43
9.4.2.2. Fraude 43
9.4.2.3. Conflicto de intereses 43
9.4.2.4. Corrupción 44
9.4.2.5. Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) - LA/FT/FP 44
9.4.3. Operación del SIGRIP 44
9.4.4. Identificación de riesgos. 45
9.4.5. Identificación de áreas de impacto 46
9.4.6. Identificación de áreas de factores de impacto. 46
9.4.7. Estructura de la Descripción del riesgo. 47
10. MONITOREO, SEGUIMIENTO Y EVALUACIÓN DE LOS MAPAS DE RIESGOS 48
11. ACCIONES POR SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO 50
12. INDICADORES CLAVE DE RIESGO 51
13. GESTIÓN DE OPORTUNIDADES 52
13.1. Identificación de Oportunidades 52
13.2. Calificación De Oportunidades 53

13.3. Escenario de Intervención 54
13.4. Desarrollo de la actividad 54
13.5. Reporte y Monitoreo 55
14. BIBLIOGRAFÍA 57
15. CONTROL DE CAMBIOS 57
16. AUTORIZACIONES 62
ANEXO 1 57

LISTA DE TABLAS

Tabla 1. Roles y responsabilidades 10
Tabla 2. Componentes y principios evaluables modelo de madurez 14
Tabla 3. Direccionamiento estratégico de la Gestión del Riesgo 16
Tabla 4.Distribución DOFA. 20
Tabla 5.Factores de riesgo 21
Tabla 6. Determinación de la probabilidad 24
Tabla 7. Determinación del impacto 24
Tabla 8. Atributos del control. 28
Tabla 9. Factores de riesgos de Gestión. 31
Tabla 10. Tabla de amenazas comunes. 33
Tabla 11. Tabla de Vulnerabilidades Comunes. 35
Tabla 12. Pasos para la identificación del riesgo fiscal 38
Tabla 13. Ejemplos de Riesgo Fiscal. 41
Tabla 14, Factores de riesgo integridad pública. 46
Tabla 15, Estructura del riesgo de integridad pública. 47
Tabla 16. Reporte de mapas de Riesgo. 48
Tabla 17. Acciones en caso de materialización. 50
Tabla 18. Matriz de Oportunidades Institucionales. 53
Tabla 19. Matriz de Oportunidades Institucionales. 53
Tabla 20. Matriz de Oportunidades Institucionales. 53
Tabla 21. Matriz de Oportunidades Institucionales. 53
Tabla 22. Matriz de Oportunidades Institucionales. 54
Tabla 23. Matriz de Oportunidades Institucionales. 54
Tabla 24. Acciones y responsabilidades Gestión de Oportunidades. 55
Tabla 25. Puntos de riesgo fiscal. 58

LISTA DE ILUSTRACIONES

Ilustración 1. Metodología para la Administración de Riesgos 15
lustración 2. Mapa de Calor de Riesgos. 15
Ilustración 3. Cadena de valor. 18
Ilustración 4. Características de un objetivo. 19
Ilustración 5. Matriz DOFA. 20
Ilustración 6. Estructura del Riesgo. 22
Ilustración 7. Ejemplo descripción de riesgo. 22
Ilustración 8. Valoración del Riesgo. 23
Ilustración 9. Severidad del riesgo. 23
Ilustración 10. Mapa de calor de Severidad 25
Ilustración 11. Riesgo residual. 25
Ilustración 12. Estructura del control. 26
Ilustración 13. Tipologías de control. 27
Ilustración 14. Desplazamiento Mapa de calor. 29
Ilustración 15. Tratamiento del Riesgo. 30
Ilustración 16. Pasos para la identificación y valoración de activos 33
Ilustración 17. Pasos para la identificación del riesgo fiscal 37
Ilustración 18. Estructura del riesgo. 40
Ilustración 19. Estructura del Riesgo Fiscal 40
Ilustración 20. Estructura del SIGRIP 45

1. INTRODUCCIÓN

La Gestión del Riesgo para el Jardín Botánico José Celestino Mutis – JBJCM, se constituye en la estrategia gerencial que le permite actuar de forma proactiva y preventiva para enfrentar cualquier evento, contingencia y oportunidad que se pueda presentar en el desarrollo de la gestión y afecte negativa o positivamente el cumplimento de los resultados esperados en la Entidad.

La política para la Gestión Integral de Riesgos tiene como propósito, otorgar criterios orientadores para la gestión y la aplicación del enfoque basado en riesgos, que permita suministrar los lineamientos conceptuales de valoración, para determinar prioridades en la atención y respuesta junto a las opciones para tratar y manejar los riesgos con base en su nivel, permitiendo compartir, evitar, reducir o asumir el riesgo, o promover la adopción de las oportunidades identificadas por los procesos.

El JBJCM define su Política para la Gestión Integral Riesgos, en el marco del Modelo Integrado de Gestión y Desempeño – MIPG y los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas (V7) del departamento Administrativo de la Función Pública - FP; el Modelo de Seguridad y Privacidad de la Información – MinTIC, Anexo 4, los “Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas” del Ministerio de Tecnologías de la Información y las Comunicaciones – TICs, a su vez se actualizan los conceptos para los Riesgos de Integridad pública de acuerdo con las directrices de la Secretaría de Transparencia de la Presidencia de la República. Así como la metodología de valoración de riesgos integrando la identificación y gestión de oportunidades, bajo los requisitos de la norma ISO: 9001:2005 para la Gestión de la Calidad.

La actualización de la Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7 que fue emitida durante el segundo semestre de la vigencia 2025, impulsa los siguientes aspectos:

1. Se mantiene estructura conceptual y metodológica general para la gestión del riesgo bajo un enfoque integral, atendiendo las políticas de gestión y desempeño que se vinculan y su relación con otras políticas públicas y los sectores que las lideran.
2. Se define una estructura de administración general para la gestión integral del riesgo, con elementos comunes aplicables a todas las tipologías de riesgo.
3. Se amplían los términos y definiciones en concordancia con la aplicación de los nuevos elementos.
4. Se profundiza el análisis sobre apetito del riesgo en el marco COSO-ERM (2017) que precisa y profundiza los conceptos de riesgo, gestión del riesgo y niveles de madurez del riesgo.
5. Se precisan contenidos conceptuales y ejemplos relacionados con la gestión preventiva de riesgos fiscales.
6. Se modifica y actualiza el capítulo de riesgos asociados a posibles actos de corrupción, incorporando el Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, de acuerdo con el componente programático de la Estrategia Institucional para la Lucha Contra la Corrupción, temática 1 Administración del Riesgo indicado en el Anexo Técnico de los Programas de Transparencia y Ética Pública.
7. Se actualizan contenidos relacionados con los riesgos de seguridad de la información, desplegando la totalidad de los pasos metodológicos.
8. Indicador Clave de Riesgo (KRI) monitorear señales tempranas de exposición al riesgo

2. OBJETIVO

Establecer los lineamientos estratégicos, el marco general y operativo que orienten la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos en el Jardín Botánico José Celestino Mutis – JBJCM que puedan afectar el logro de los objetivos institucionales, en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG) y las mejores prácticas internacionales de gestión de riesgos basadas en el marco COSO ERM. Con el propósito de fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público, asegurando la integridad, transparencia y eficiencia en la administración de recursos. Igualmente, busca promover una cultura organizacional orientada a la anticipación y gestión proactiva de riesgos, contribuyendo al cumplimiento de la misión institucional, la mejora continua, la confianza ciudadana en Bogotá y la protección de la integridad pública.

Lo anterior contemplando la relación con los diferentes grupos de valor con los que la entidad se relaciona, especialmente las contrapartes; las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización; los procesos, servicios, trámites u otras operaciones administrativas de la organización, especialmente aquellas que implican alguna interacción y las jurisdicciones o territorios donde se opera.

3. ALCANCE

Se inicia con la manifestación de la Política junto al suministro de la metodología para la Gestión integral del Riesgo contemplando todas las etapas de aplicación, continua con los espacios de autocontrol, , monitoreo, seguimiento y evaluación bajo el esquema de las líneas de defensa y el Modelo de operación por procesos, y finaliza con la retroalimentación y toma de decisiones con base en los resultados obtenidos para cada una de las tipologías de riesgos permitiendo el análisis y mejora continua de las actuaciones efectuadas por las partes aplicando el enfoque basado en riesgos.

La aplicabilidad de los riesgos de Gestión, Fiscales, Seguridad de la Información, Integridad Pública y la Gestión de Oportunidades, parte desde el direccionamiento estratégico, la aplicación del modelo de operación por procesos, el desarrollo de los planes y políticas institucionales, así como los proyectos y demás sistemas de gestión establecidos e implementados en el JBJCM.

La presente política aplica a todas las dependencias, procesos, servidoras y servidores de la entidad, en todos los niveles jerárquicos y áreas misionales, estratégicas y de apoyo. Incluye la gestión de riesgos en la planeación, ejecución presupuestal, prestación de servicios, adopción de tecnologías, fortalecimiento organizacional, así como en la implementación de proyectos y programas institucionales.

4. NORMATIVIDAD

La normatividad asociada al desarrollo de este documento se encuentra en el Normograma del Jardín Botánico José Celestino Mutis - JBJCM.

5. MARCO CONCEPTUAL

Activo (CONPES 3854:2016, pág.56): Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y

administrativa. 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.

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

Análisis Del Riesgo: Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

Áreas de Impacto: Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son económicos y reputacionales.

Atributos de eficiencia: Corresponde a las características que determinan la tipología (Preventivo, Detectivo, Correctivo) y mecanismo de implementación (Automático o Manual) de los controles. Estos atributos poseen un peso que permite determinar el porcentaje de eficiencia al confirmar su ejecución.

Atributos informativos: Permiten darle formalidad al control y su fin es el de conocer el entorno de este complementando el análisis con elementos cualitativos; sin embargo, no tienen una incidencia directa en su efectividad.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. (relacionado con la solvencia y liquidez).

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Control: Medida que permite reducir o mitigar un riesgo. Los responsables de implementar y monitorear los controles son los dueños de proceso.

Control Correctivo: Acción que se ejecuta después de que se materializa el riesgo y en la mayoría de las ocasiones permiten reducir el impacto de dicho 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 Preventivo: Acción y/o mecanismo ejecutado antes que se realice la actividad originadora del riesgo, que busca establecer condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.

Corrupción: Práctica deshonesta que implica el abuso de poder para obtener beneficios personales ilegítimos, a menudo en detrimento de la integridad y ética organizacional.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Gestión del Riesgo: Proceso efectuado por la Alta Dirección de la Entidad y por todo el personal, para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. Se integra en el desarrollo de la estrategia, la formulación de los objetivos de la Entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana.

Gestión de Oportunidades: Aspectos positivos externos a los procesos y de las partes interesadas que podrían aprovecharse con el fin de convertirlos en fortalezas y así poder contribuir a la prestación de los servicios proporcionados a los ciudadanos del Distrito Capital.

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)4" . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

Impacto: Las consecuencias negativas o positivas que puede ocasionar a la organización la materialización del riesgo u oportunidad.

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.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden Nacional, Departamental y Municipal.

Probabilidad: Se entiende como 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.

Puntos de Riesgo: Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Riesgo de Integridad Pública: Amenazas que pueden incidir en diferentes puntos de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en particular, asegurar el cumplimiento de la ley.

Riesgo de Gestión: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. 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 Lavado de Activos y Financiación del Terrorismo – LA/FT: Se define como la posibilidad de pérdida o daño que puede sufrir una entidad por su propensión a ser utilizada directamente o a través de sus operaciones, como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

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: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial[1].

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

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

SARLAFT: Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo.

Severidad: Nivel de un riesgo, dado por una probabilidad y un impacto. En cada nivel se define el tratamiento y los niveles de responsabilidad.

SIGRIP: Sistema de Gestión de Riesgos para la Integridad Pública en el que se contempla que la entidad adopte una serie de instrumentos de gestión del riesgo, que actúe con diligencia en el conocimiento de sus contrapartes y que integre en su operación una función de cumplimiento, todo esto además de la identificación y valoración de los riesgos según la metodología definida en la Política para la Gestión Integral de Riesgos.

Soborno: Consiste en un ofrecimiento, promesa, entrega, aceptación o exigencia de un incentivo para realizar una acción ilícita, antiética o que supone abuso de confianza. Los incentivos pueden consistir en obsequios, préstamos, comisiones, recompensas u otras ventajas (impuestos, servicios, donaciones, etc.)

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.

6. RESPONSABLES Y ROLES

En el marco del Modelo Integrado de Planeación y Gestión, la Política para la Gestión Integral de Riesgos desarrolla el esquema de las Líneas de Defensa, como eje articulador de la gestión y control de la Entidad, cuyo propósito es establecer los roles y responsabilidades en todas las instancias y niveles frente al riesgo y el control. En tal sentido, el JBJCM ha determinado la distribución de responsabilidades de la siguiente manera:

[1] *Concepto propuesto por Función Pública, a partir del análisis de fallos de responsabilidad fiscal y literatura investigada sobre el tema*

Tabla 1. Roles y responsabilidades

LINEA ESTRATEGICA	
Responsable	**Roles**
Director (a) General - Comité Institucional de Coordinación de Control Interno-CICCI	Establecer las políticas de operación encaminadas a controlar los riesgos y oportunidades que pueden llegar a incidir en el cumplimiento de los objetivos institucionales
	Establecer y monitorear los estándares de conducta y de integridad, que direccionan el que hacer institucional.
	Determinar y mantener bajo seguimiento el nivel de aceptación del riesgo para los Riesgos de Gestión, Riesgos de integridad pública, Riesgos Fiscales y de Seguridad de la Información.
	Monitorear los resultados de los riesgos identificados y gestionados que permiten asegurar el cumplimiento de los objetivos.
	Aprobar la Política para la Gestión Integral del Riesgos y monitorear su cumplimiento.
	Aprobar el Plan Anual de Auditoría propuesto por el Jefe de la Oficina de Control Interno o quien haga sus veces.
	Establecer los lineamientos para el funcionamiento y evaluación del estado del Sistema de Control Interno.
	Asegurar un ambiente de control que le permita a la Entidad disponer de las condiciones mínimas para el ejercicio del control interno.
	Establecer los lineamientos para la identificación, disponibilidad, captura y comunicación de la información confiabilidad, integridad y seguridad de la información.
	Analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP
PRIMERA LINEA DE DEFENSA	
Líderes de Proceso, enlace MIPG y Equipo de Trabajo	Efectuar la identificación, definición, valoración, ejecución, seguimiento y autoevaluación de la efectividad de los controles y/o acciones definidas para su tratamiento, conforme a lo establecido en la Política para la Gestión Integral de Riesgos para Riesgos de Gestión, Riesgos de integridad pública, Riesgos Fiscales y Seguridad de la Información, así como la Gestión de Oportunidades y lo establecido para los activos de información en las herramientas indicadas por la segunda línea de defensa para cada tipología.
	Cada proceso cuenta con un designado que apoya las etapas de la gestión integral del riesgo como enlace entre la primera y segunda línea de defensa.
	En concordancia con la cultura del autocontrol, debe: actualizar y diseñar, monitorear y evaluar permanentemente la Gestión del Riesgo permitiendo su mitigación proponiendo mejoras.
	Cumplir con las políticas y lineamientos para comunicar la información a nivel interno y externo que facilita el funcionamiento del Sistema de Control Interno - SCI de la Entidad.
	Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y su respectivo plan de acción.
	Reportar los avances de la Gestión de los Riesgos (gestión, Riesgos de integridad pública, fiscales y seguridad de la información) dentro de los plazos establecidos por la segunda línea de defensa mediante evidencia objetiva.
	Revisar en cada vigencia y/o por su solicitud, la formulación y tratamiento de los riesgos con el fin de establecer un manejo adecuado de los mismos desde la planeación y contribuir así al logro de los objetivos institucionales y del proceso, teniendo en cuenta las observaciones y oportunidades de mejora evidenciadas por la segunda y tercera línea de defensa

	Les corresponde la ejecución y el monitoreo de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.
SEGUNDA LINEA DE DEFENSA	
Oficina Asesora de Planeación	Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la Política para la Gestión Integral de Riesgos y el establecimiento de los niveles de impacto, así como orientar y apoyar en la formulación y consolidación de los mapas y matrices de riesgos en el JBJCM.
	Consolidar los Mapas Institucionales de Riesgos de Gestión, Riesgos de integridad pública, Fiscales y Seguridad de la Información, así como la Gestión de Oportunidades, y presentarlo para análisis y seguimiento ante el CICCI, en las herramientas establecidas para cada tipología.
	En el marco de la Política para la Gestión Integral de Riesgos, realizar monitoreo a la adecuada identificación y tratamiento de los riesgos establecidos por la primera línea de defensa en los Mapas de Riesgos de Gestión, Riesgos de integridad pública, Fiscales y Seguridad de la Información, así como la Gestión de Oportunidades.
	Verificar que los controles contribuyen en la prevención, detección y/o corrección frente a la materialización de los distintos tipos de riesgos identificados, así como supervisar la implementación de prácticas de gestión de riesgo eficaces.
	Acompañar a los procesos en la revisión en cada vigencia y/o por su solicitud en la formulación y tratamiento de los riesgos con el fin de establecer un manejo adecuado de los mismos desde la planeación y contribuir así al logro de los objetivos institucionales y de los procesos, teniendo en cuenta las observaciones y oportunidades de mejora evidenciadas por la segunda y tercera línea de defensa
	El Proceso de Seguridad de la Información – SDI es el encargado de apoyar en conjunto a los procesos respecto a la identificación de los riesgos de seguridad de la información digital, a partir de los activos de información, para la valoración y tratamiento de los Riesgos de Seguridad de la Información, así como el diseño, desarrollo, implementación y control del Modelo de Seguridad Digital (MSPI).
Equipo de cumplimiento	Establecidos en la Política DYP.PO.06 SARLAFT.
TERCERA LINEA DE DEFENSA	
Oficina de Control Interno - OCI	Realizar el seguimiento y evaluación de la Gestión de los Riesgos de Gestión, Riesgos de integridad pública, Fiscales y Seguridad de la Información, así como la Gestión de Oportunidades, de acuerdo con la normatividad vigente y/o el Plan Anual de Auditoría Interna de la vigencia.
	Realizar seguimiento al cumplimiento del presente procedimiento según lo programado en el Plan Anual de Auditoría Interna de la vigencia.
	Asesorar de forma coordinada con la Oficina Asesora de Planeación, a la primera línea de defensa en la identificación y tratamiento de los riesgos institucionales y diseño de controles.
	Auditar el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP y el cumplimiento de la presente política, así como sus complementos, con el propósito de asesorar y recomendar mejoras.

Fuente: Elaboración propia OAP.

7. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El JBJCM asume el compromiso de administrar los Riesgos de Gestión, Riesgos de integridad pública, Riesgos de Seguridad de la Información y Riesgos Fiscales; que puedan afectar de manera negativa el alcance de los objetivos estratégicos y los objetivos de los procesos de la entidad; además de forjar una entidad preventiva, proactiva y detectiva en lugar de reactiva y correctiva, que trabaje en la reducción de los efectos no deseados y promoviendo la mejora continua, proyectando así, una

organización basada en la acción preventiva automática, que controla todos los procesos de la entidad, brindando seguridad razonable, destinando los esfuerzos y recursos necesarios para administrar los riesgos y la definición de la ruta estratégica y operativa con el propósito de satisfacer las necesidades de los grupos de valor.

Lo anterior, fundamentado en la determinación de la capacidad del riesgo, el nivel de apetito del riesgo y la tolerancia del riesgo.

La administración del riesgo se complementa con la gestión de las oportunidades, donde se identifican las situaciones positivas que los procesos deben aprovechar para mejorar el desempeño y acciones proyectadas.

La entidad adopta los siguientes valores clave respecto a la Gestión Integral del Riesgo:

- Integrada: Es parte integral de todas las actividades de la organización.
- Estructurada y exhaustiva: Posee un enfoque estructurado y exhaustivo contribuyendo a resultados coherentes y comparables.
- Adaptada/Ajustada: El marco de referencia y su proceso se adaptan y son proporcionales al contexto interno y externo de la organización relacionados con sus objetivos.
- Inclusiva: La participación apropiada y oportuna de las partes interesadas permite que se considere su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una administración informada.
- Dinámica: Los riesgos pueden aparecer, cambiar o desaparecer con los cambios del contexto interno y/o externo de la organización, permitiendo anticipar, detectar, reconocer y responder a esos cambios y eventos de una manera apropiada y oportuna.
- Mejor información disponible: Las entradas se basan en información histórica y actualizada, así como en expectativas, tiene en cuenta las limitaciones e incertidumbres asociadas con tal información y expectativas. La información es oportuna, clara y disponible para las partes interesadas pertinentes.
- Factores humanos y culturales: El comportamiento humano y la cultura influyen considerablemente en sus aspectos, niveles y etapas.
- Mejora continua: Mejora continuamente mediante el aprendizaje, la experiencia y los resultados obtenidos al finalizar cada periodo de seguimiento permitiendo fortalecerse, se debe analizar la continuidad de cada riesgo como mínimo una vez al año en mesa de trabajo entre el proceso responsable y la Oficina Asesora de Planeación.
- Actualizada: Los procesos son los responsables de requerir la actualización de los riesgos de acuerdo con la realidad operativa, el ejercicio se debe efectuar con el apoyo metodológico de la Oficina Asesora de Planeación y debe registrarse mediante Acta de reunión reflejando los ajustes en el Mapa Institucional de Riesgos.

8. RUTA DE IMPLEMENTACIÓN

8.1. Metodología para la Gestión Integral del Riesgo

Para el desarrollo de una óptima gestión del riesgo la entidad adopta la estructura sugerida por COSO-ERM-2017 (*Committee of sponsoring organizations of the treadway Commission – Enterprise Risk Management* por sus siglas en inglés), descrita en la "*Guía para la Gestión Integral del Riesgo en Entidades Públicas"* versión 7 del Departamento Administrativo de la Función Pública, que manifiesta

5 componentes que integran la óptima gestión del riesgo y son desarrollados de la siguiente a continuación:

a. Gobierno y Cultura:

Son la base de los demás componentes, mediante el gobierno se indican los lineamientos, manifestando la importancia y suministrado los roles y responsabilidades frente a la gestión integral del riesgo. La cultura es reflejada en la toma de decisiones al interior de la entidad dados los monitoreos y seguimientos.
Para lo anterior desde el Comité Institucional de Coordinación de Control Interno – CICCI se ejercerá la supervisión de la gestión integral del riesgo, se debe cumplir con la estructura operativa descrita en el capítulo 6 “Roles y Responsabilidades”, la cultura deseada se obtiene dada la aplicación de la presente Política frente a la gestión del riesgo, se desarrollan el compromiso con los valores clave descritos en el numeral 7. “Principios Orientadores”, y propende la atracción, desarrollo y retención de profesionales capacitados.

b. Estrategia y establecimiento de Objetivos:

La gestión integral del riesgo se integra con el plan estratégico de la entidad a través del establecimiento de la estrategia y de los objetivos de la entidad. Con un conocimiento profundo del contexto de la entidad y de los procesos, se comprenden los factores internos y externos y sus efectos en el riesgo. En su desarrollo se analiza el contexto estratégico, se logra la definición del apetito del riesgo, se evalúan las estratégicas de gestión y se formulan los objetivos del negocio.

c. Desempeño

La entidad identifica y evalúa los riesgos que pueden afectar su capacidad para alcanzar los objetivos estratégicos y de proceso. Por lo anterior se establecen las respuestas a los eventos de riesgo y efectúa monitoreo y seguimiento al desempeño considerando posibles cambios mediante la toma de decisiones. En su desarrollo se efectúa la identificación de los riesgos, se evalúa su gravedad estableciendo prioridades, así como implementando respuesta ante los eventos fortaleciendo la visión de la gestión.

d. Revisión y monitorización

La entidad examina sus capacidades y lineamientos respecto a la gestión integral del riesgo, así como su desempeño en relación con sus objetivos permitiéndose evaluar los cambios significativos, revisando los eventos y los resultados de sus seguimientos, promoviendo la mejora.

e. Información, comunicación y reporte

Corresponde al proceso continuo e iterativo de obtener y compartir información en toda la entidad. La Alta Dirección utiliza información obtenida por los informes de monitoreo y seguimiento (fuentes internas) y los suministrados por auditorías externas para facilitar la gestión integral del riesgo. La entidad aprovecha los sistemas de información para capturar, procesar y gestionar datos e información. Al utilizar información que se aplica a todos los componentes, la organización informa sobre el riesgo, la cultura y el desempeño.

8.2. Determinación del Nivel de madurez

Para determinar el nivel de madurez se deben evaluar los componentes y los principios descritos previamente y reflejados en la tabla 2, ejercicio que obtiene asignando una calificación de 1 a 5 para cada uno de los principios, permitiendo obtener el grado de madurez para la gestión integral del riesgo en la entidad. Para el desarrollo del ejercicio se cuenta con el "Autodiagnóstico madurez Gestión Integral del Riesgo", herramienta suministrada por el Departamento Administrativo de la Función Pública y que es apropiado por la entidad que consolida los resultados por componente y genera un mapa de calor, donde se resaltan los temas a intervenir en una escala de severidad o prioridad para atención, de tal manera que la Oficina Asesora de Planeación informa a la Alta Dirección en el CICCI las orientaciones o acciones que desde allí deben surgir para garantizar la gestión integral del riesgo en la entidad.

Tabla 2. Componentes y principios evaluables modelo de madurez

Componente	Principios
Gobierno y Cultura	Supervisión de riesgos a través del consejo de administración
	Establece estructuras operativas
	Define la cultura deseada
	Demuestra compromiso con valores clave
	Atrae, desarrolla y retiene a profesionales capacitados
Establecimiento de la estrategia y objetivos	Analiza el contexto (externo e interno)
	Define el apetito del riesgo
	Evalúa estrategias alternativas
	Formula objetivos estratégicos y operacionales
Desempeño	Identifica y describe el riesgo
	Evalúa el riesgo inherente
	Diseña controles efectivos
	Prioriza riesgos
	Desarrolla visión integral
Análisis y monitorización	Evalúa los cambios significativos
	Revisa el riesgo y el desempeño
	Persigue la mejora de la gestión del riesgo
Información, Comunicación y Reporte	Aprovecha la información y la tecnología
	Comunica información sobre riesgos
	Informa sobre el riesgo, la cultura y el desempeño

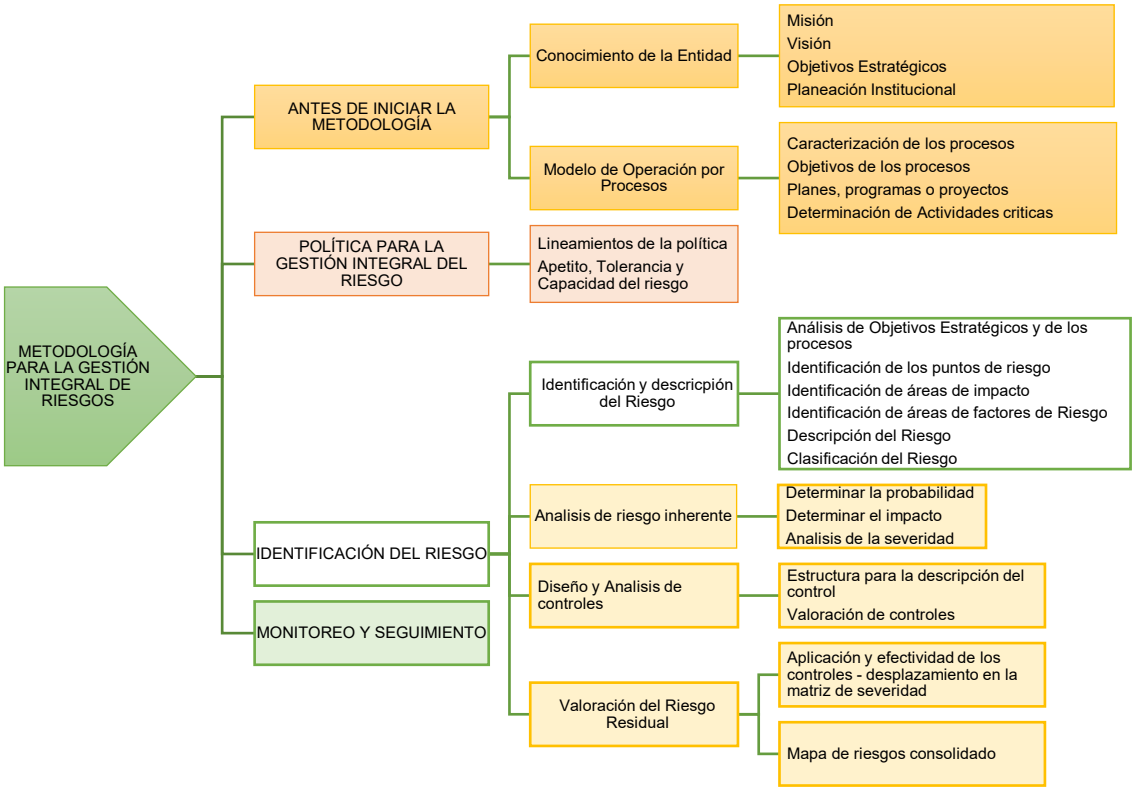
Fuente: Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

El análisis sobre niveles de madurez debe desarrollarse una vez al año.

8.3. Metodología para la Gestión Integral del Riesgo

Para la adecuada gestión integral del Riesgo el JBJCM establece el desarrollo de las siguientes etapas que son desarrolladas en la presente política:

Ilustración 1. Metodología para la Administración de Riesgos

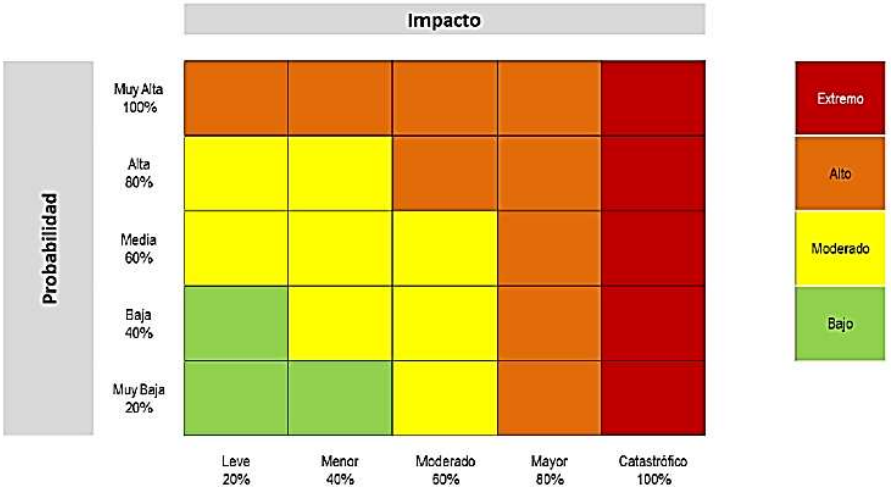


Fuente: Elaboración propia OAP.

8.4. Apetito, Tolerancia y Capacidad del Riesgo.

Para ilustrar el Apetito del Riesgo, Tolerancia del Riesgo y Capacidad del Riesgo determinado por el JBJCM es necesario revisar gráficamente el Nivel del Riesgo en el mapa de calor, lo cual se detalla a continuación:

lustración 2. Mapa de Calor de Riesgos.



Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

Para ello, es necesario aclarar que la entidad hace uso del mapa de calor sugerido por Función Pública, en este el Nivel del Riesgo 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. Dado lo anterior, se establece lo siguiente:

Tabla 3. Direccionamiento estratégico de la Gestión del Riesgo

CONCEPTO	NIVEL DE RIESGO
Apetito del Riesgo	Nivel de Riesgo **Bajo**.
Tolerancia del Riesgo	Desde nivel de Riesgo **Moderado** hasta Nivel de Riesgo **Alto**.
Capacidad de Riesgo	Nivel de Riesgo **Extremo**.

Fuente: Elaboración propia OAP.

La Alta Dirección considera que el nivel de riesgo extremo es el valor máximo que, podrá ser resistido por la Entidad, manteniendo la capacidad de cumplir con sus objetivos trazados. En caso de evidenciar eventos de riesgo que sobrepasen el nivel de riesgo extremo requerirán su replanteamiento incluyendo la posibilidad de definir nuevos valores de probabilidad e impacto.

Nota: En todo caso para los riesgos identificados e incluidos en las matrices de Riesgos se deben formular acciones de tratamiento.

8.5. Identificación de riesgos.

Son varios los insumos para efectuar la identificación de riesgos, dentro de los elementos que se deben tener en cuenta se encuentran los siguientes: el contexto estratégico en el que opera la entidad y los procesos contemplando los factores internos y externos, la caracterización de cada proceso y el desarrollo de sus actividades críticas contemplando su objetivo y alcance, y finalmente el análisis de los objetivos estratégicos de la entidad y del proceso.
Se recomienda el uso de al menos uno de ellos, sin embargo, para poder establecer una adecuada identificación del Riesgo dichos elementos deben combinarse.

A) Análisis de Factores de Riesgo

En esta etapa se deben tener en cuenta:

- **Contexto externo:** Se examinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:
  - Políticos.
  - Económicos y financieros.
  - Sociales y culturales.
  - Tecnológicos.
  - Ambientales.
  - Fiscal.
  - Legales y reglamentarios.
  - Grupos de interés externos y partes interesadas.
  - Clientes, proveedores de servicio y empresas.
  - Cantidad de ciudadanos afectados por la falta del servicio.

- Suplantación de identidad.
- Asaltos/Vandalismo/Ataque terrorista/Orden Público a las instalaciones de la entidad.
- Resultados de las evaluaciones llevadas a cabo por los organismos de control.

- **Contexto interno:** Se analizan cuáles son los rasgos distintivos que dictan la manera en la cual opera internamente y busca alcanzar sus objetivos institucionales:
  - Sector.
  - Misión.
  - Visión.
  - Valores.
  - Estructura organizacional.
  - Funciones y responsabilidades.
  - Políticas, procesos y procedimientos. Objetivos y estrategias implementadas.
  - Sistema de gestión.
  - Recursos y conocimientos con que se cuenta (económicos, social, ambiental, físico, financiero, jurídico, Humano, procesos, sistemas, infraestructura física y tecnológica, información, Seguridad Digital).
  - Relaciones con las partes involucradas y grupos de valor.
  - Cultura organizacional.
  - Infraestructura.
  - Tramites u otros procedimientos administrativos - OPA´S.
  - Resultados de las evaluaciones llevadas a cabo por la OCI.

- **Contexto del Proceso:** Se revisan cuáles son las características o aspectos esenciales del proceso, si está directamente relacionado con un objetivo estratégico de la entidad, cuál es su alcance, cuáles son las entradas y las salidas derivadas de las actividades que se realizan en su interior:
  - Objetivo del proceso.
  - Alcance del proceso.
  - Caracterización del proceso.
  - Interrelación con otros procesos.
  - Procedimientos asociados.
  - Responsables del proceso.
  - Cantidad de ciudadanos afectados por el proceso.
  - Procesos de gestión de riesgos actualmente implementados.
  - Actividades criticas

- SIGRIP: En cumplimiento a la implementación se deben realizar los siguientes análisis:
  - La planta y estructura de la entidad, así como la delegación de autoridad o poder decisorio discrecional.*
  - Los grupos de valor o partes interesadas, incluidos los clientes internos y externos, permitiendo la identificación de contrapartes, es decir, partes con las que se tienen interacciones, entendidas estas como cualquier tipo de vinculación que involucre la prestación o entrega de un producto, o el intercambio de recursos.
  - Identificar los lugares en qué opera la entidad.
  - La naturaleza, escala y complejidad de los procesos, servicios, trámites u otras operaciones administrativas de la organización, así como las interacciones, es decir, las operaciones con contrapartes que involucran la prestación o entrega de un producto, o el intercambio de recursos.

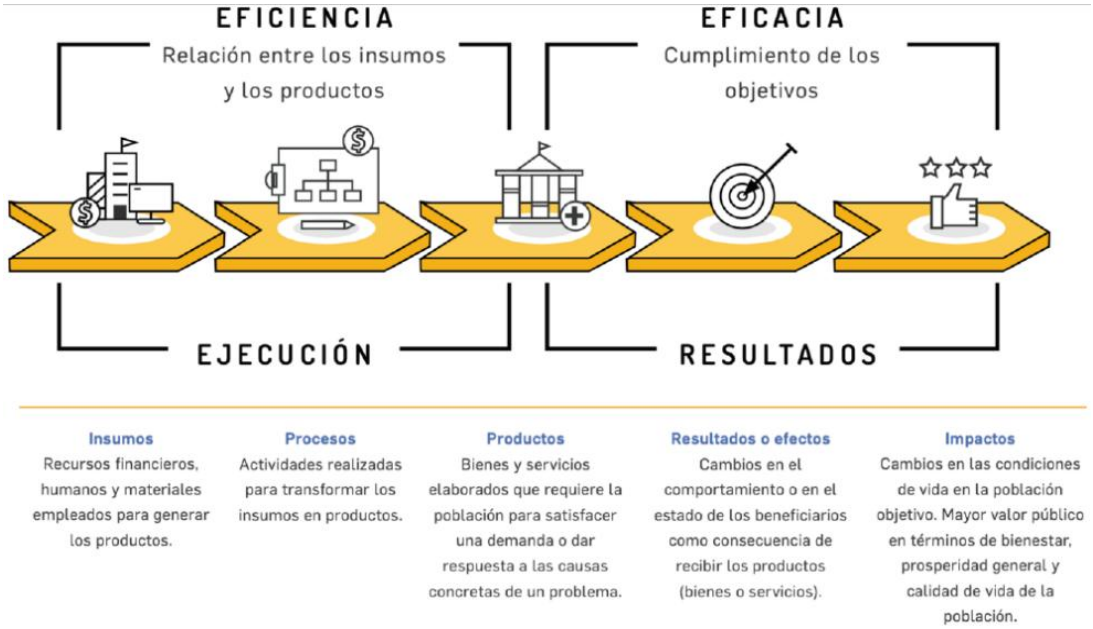
- Segmentar la información general de los contratos y principales proveedores de la entidad. Agrupar los contratos y proveedores según sus características: naturaleza jurídica, modalidad de selección más recurrente, valores mínimos, máximos y media de contratación, relación de cumplimiento o incumplimientos, tipos de supervisión, entre otras.
- Identificar las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización.*
- La naturaleza y alcance de las interacciones con entidades de otras Ramas del Poder Público, órganos de control o independientes. Así como de las interacciones con particulares que no derivan en un vínculo formal, pero que son recurrentes (actividades de cabildeo).*
- Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales. Agrupando entre aquellas que son deberes (obligatorio cumplimiento), expectativas (cumplimiento facultativo) y compromisos (cumplimiento asumido).*

* Desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.

B) Identificación y análisis de las actividades críticas del proceso

Dado que los objetivos estratégicos y de proceso se alcanzan por medio de la ejecución de actividades, en esta etapa se busca identificar las situaciones cruciales para la consecución de los objetivos validando la integridad de la caracterización del proceso y los procedimientos que lo componen, lo anterior es lo que se denomina Puntos de Riesgo dentro de la cadena de valor.

Ilustración 3. Cadena de valor.



Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

De este modo, para establecer los puntos de riesgo clave en los procesos, es necesario considerar los atributos asignados a los productos, servicios o resultados de cada proceso y que podrían verse

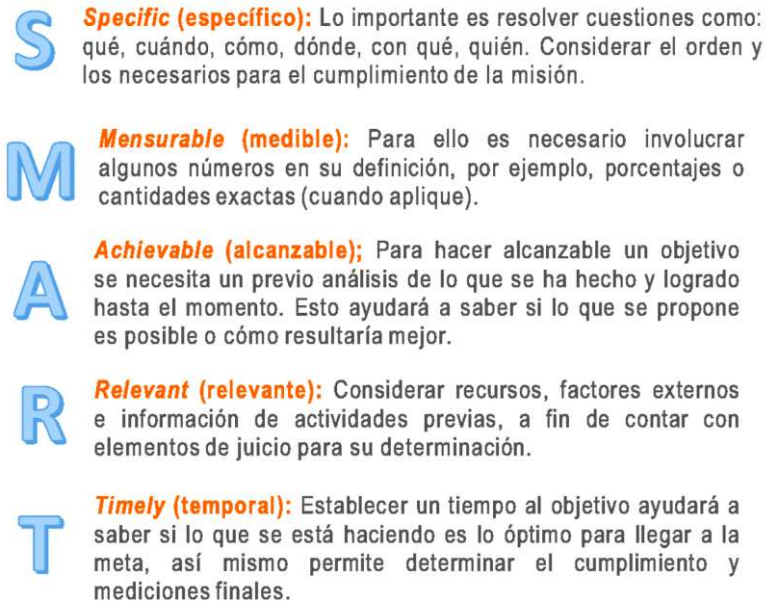
afectados dentro del ciclo del proceso que se esté analizando, así como el efecto de estos posibles eventos en el resultado de otros procesos, dentro de la cadena de valor.

C) Análisis de los Objetivos Estratégicos y de los Procesos

En una correcta construcción de objetivos por procesos se debe tener en cuenta la correlación que debe existir entre los objetivos estratégicos de la entidad y éstos, teniendo en cuenta el cumplimiento y cualquier situación que pueda representar su éxito o fracaso, a su vez, los objetivos estratégicos deben estar alineados con la misión y visión de la entidad. Lo anterior, permite una apropiada gestión de planeación en la identificación del riesgo en función de la afectación al logro y su posible fracaso impactando los propósitos de la entidad.

Un objetivo debe contar con las siguientes características:

Ilustración 4. Características de un objetivo.



Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025.

El proceso de identificación del riesgo es desarrollado por el responsable del proceso (Primera línea de defensa) y debe contar con el acompañamiento de la Oficina Asesora de Planeación (Segunda línea de defensa). En su desarrollo se deben responder las siguientes preguntas:

- ¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- ¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto.
- ¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo con el desarrollo del proceso.
- ¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo.

8.5.1. Clasificación del Riesgo por Factor

Para identificar adecuadamente los riesgos se recomienda que se lleve a cabo un análisis de matriz **DOFA** (Debilidades, Oportunidades, Fortalezas y Amenazas), esta es una técnica para ubicar los factores internos y externos identificados en la etapa previa y que afectan positiva o negativamente la forma en la cual una organización alcanza sus objetivos.

El ejercicio de la **DOFA** debe ser ejecutado en función de los objetivos estratégicos y los objetivos del proceso. Como mínimo, este ejercicio se debe realizar una vez al año y debe ajustarse las veces que sea necesario.

Ilustración 5. Matriz DOFA.

Fuente: Elaboración Propia OAP

Las **debilidades** y **fortalezas** son de carácter interno y provienen del análisis del contexto o factor internos del proceso. De otro lado, las **oportunidades** y las **amenazas** corresponden al análisis del contexto o factor externo de la entidad y del proceso.

Tabla 4.Distribución DOFA.

DEBILIDADES	OPORTUNIDADES
Contexto interno	**Contexto externo**
FORTALEZAS	**AMENAZAS**
Contexto interno	**Contexto externo**

Fuente: Elaboración Propia OAP.

8.6. Identificación de áreas de impacto

Corresponde a la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que el JBJCM adopta son afectación económica (o presupuestal) y reputacional. Los cuales se evalúan para cada evento de riesgo identificado, pueden presentarse individualmente o en conjunto.

8.7. Identificación de áreas de factores de riesgo

Comprende las fuentes generadoras de riesgos, son las circunstancias o condiciones que aumentan la probabilidad de que ocurra el evento de riesgo, bien sea fuentes interna o externa. No son causas directas de los riesgos, pero incrementan el nivel de exposición.

A continuación, en la tabla 4. se establece el listado con los factores de riesgo que pueden incidir en los procesos.

Tabla 5.Factores de riesgo

Factor	Definición	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos
		Falta segregación de funciones
		Errores de grabación, autorización
		Falta de supervisión o interventoría
		Errores en cálculos para pagos internos y externos
		Alta rotación o insuficiencia de personal
		Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
		Acciones contrarias a las leyes o acuerdos contractuales
		Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas)
		Productos (bienes o servicios) que oferta/requiere
		Canales utilizados para la operación
		Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Fraude Interno
		Soborno entrante
		Soborno saliente
		Gestión inadecuada de conflicto de Intereses
		Corrupción
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Hurto de activos
		Caída de sistemas de información y aplicaciones
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.	Fraude Externo
		Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

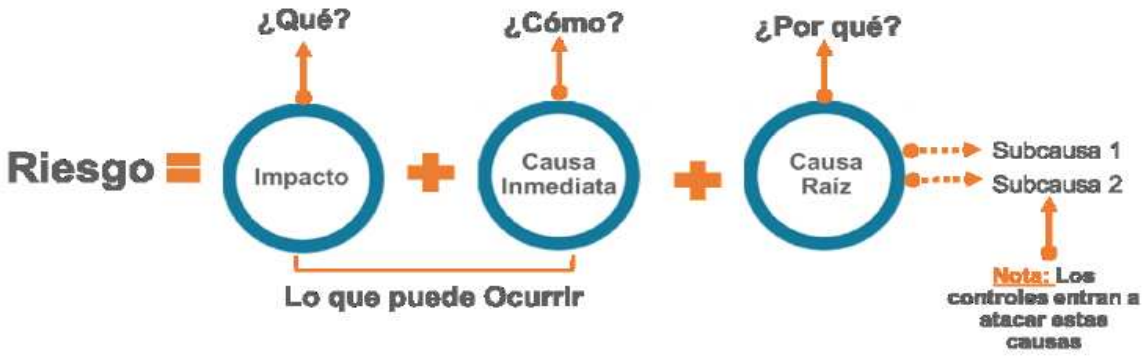
Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

8.8. Estructura de la descripción del Riesgo

Identificado lo anterior, se debe establecer la descripción del Riesgo la cual consta de la siguiente estructura impacto, causa inmediata y la causa raíz, de acuerdo con lo siguiente:

- **Impacto:** las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la entidad 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:** Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles en el paso 3 de diseño y análisis de controles. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Ilustración 6. Estructura del Riesgo.



Fuente: Elaboración propia OAP.

Estos dos primeros elementos permiten plantear el evento no deseado (¿qué puede ocurrir?), es decir la situación, acción, condición o suceso incierto que, si ocurre, podría afectar el logro de los objetivos de la entidad. Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.

El último elemento identifica la causa raíz y condiciones contribuyentes que pueden clasificarse en: humanas, tecnológicas, normativas, ambientales, organizacionales. Un adecuado análisis de causa raíz debe permitir diferenciar la causa raíz, de la causa inmediata, entendida esta última como las circunstancias más evidentes sobre las cuales se presenta el riesgo y que en ocasiones, no constituyen la causa principal del riesgo.

Ilustración 7. Ejemplo descripción de riesgo.

Ejemplo: posibilidad de afectactación económica y reputacional por incumplimientos a la gestión documental, debido a la pérdida de expedientes del archivo central.

En este caso se trata de un riesgo asociado a la gestión documental, pero esta causa raíz relacionada con la pérdida de expedientes puede representar un riesgo frente a la gestión contractual, la gestión jurídica y en cada proceso sus responsables y controles son específicos.

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) - DAFP

La descripción de los riesgos debe cumplir con lo siguiente:

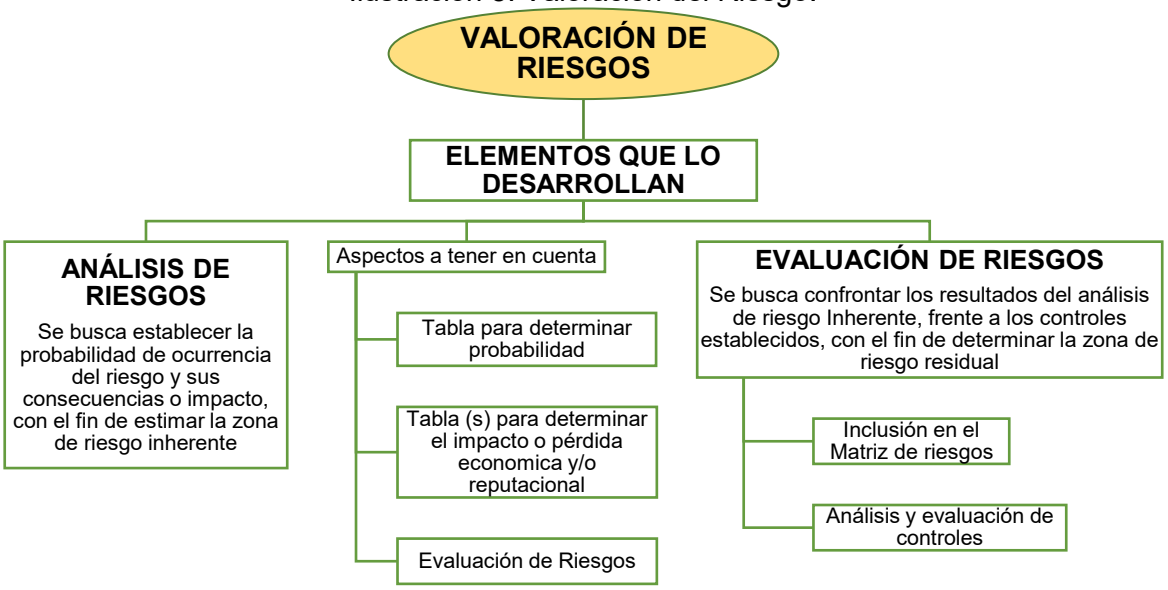
- Los riesgos no se deben describir como fallas ni desviaciones de los controles.
- Evitar describir riesgos como la negación del control.
- No existen riesgos transversales, lo que puede existir son causas transversales.

8.8.1. Valoración del Riesgo

En esta etapa se busca determinar la probabilidad de ocurrencia y el nivel de consecuencia o impacto del riesgo para la entidad, como resultado se obtiene la zona de riesgo inherente, posteriormente los eventos son confrontados con la formulación de controles que permitan afrontar las causas detectadas permitiendo efectuar tratamiento y representar como resultado la zona de riesgo residual.

El escenario de valoración del riesgo se refleja de la siguiente manera:

Ilustración 8. Valoración del Riesgo.



Fuente: Elaboración Propia

8.8.2. Análisis del Riesgo Inherente

En esta etapa se determina el Riesgo Inherente (sin ningún tipo de aplicación de controles), a partir de la combinación de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, estableciendo el nivel de severidad.

Ilustración 9. Severidad del riesgo.

Fuente: Elaboración propia

Para tal fin, se utilizan los criterios establecidos en las siguientes tablas para medir el nivel de probabilidad y el impacto:

Tabla 6. Determinación de la probabilidad

	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces al 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 5.000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año	100%

Fuente: Elaboración propia

Se entiende como probabilidad a la posibilidad de ocurrencia del riesgo, en tal sentido estará asociada a la exposición al riesgo de la actividad que se esté analizando. De este modo, la probabilidad es el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Tabla 7. Determinación del impacto

	Afectación Económica	Probabilidad
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 acciones y/o de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

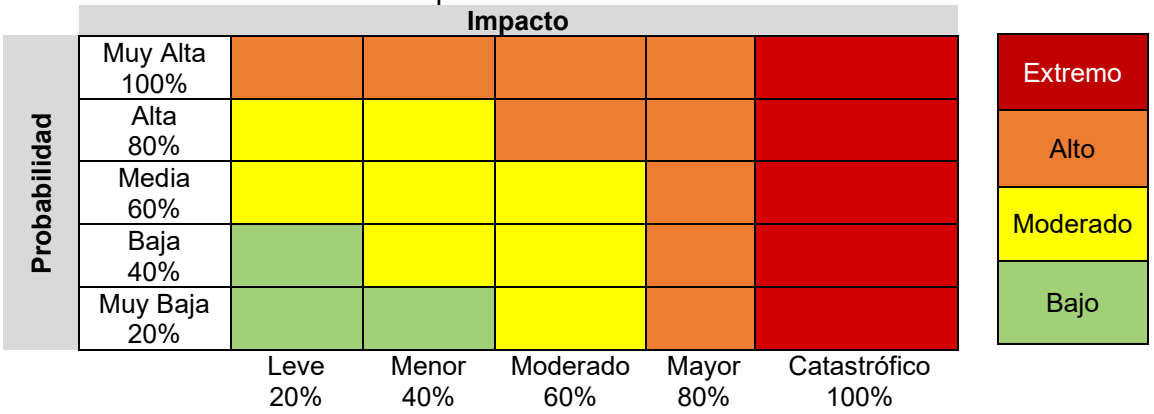
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (V6) – DAFP

El impacto está asociado a las consecuencias que puede ocasionar el riesgo a la entidad por la materialización de un riesgo. Se asumen criterios de impacto económico y/o reputacional como las variables a evaluar. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel mayor e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel mayor.

8.8.3. Zonas de severidad

La entidad establece para todas las tipologías de riesgo el siguiente mapa de calor en el cual se reflejan 4 zonas de severidad a razón de la probabilidad e impacto determinadas. Con la valoración del riesgo se determina su ubicación grafica en el mapa permitiendo obtener un apoyo grafico sobre el nivel de riesgo inherente permitiendo la toma decisiones individual o en conjunto con los demás riesgos valorados del proceso y de la entidad.

Ilustración 10. Mapa de calor de Severidad

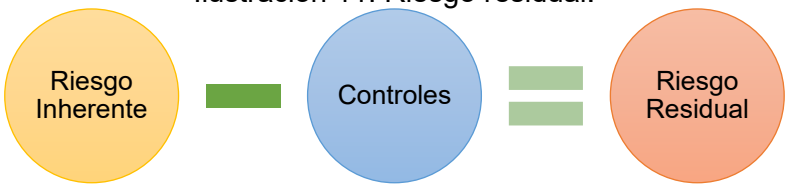


Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) - DAFP

8.9. Diseño, Análisis y Valoración de Controles

Luego de establecer el nivel de riesgo inherente se requiere la formulación de acciones concretas con atributos específicos con el propósito razonable que permita mitigar la posible materialización del riesgo detectado y por ende posible incumplimiento de los objetivos trazados. Esta etapa tiene como propósito tomar como punto de partida el nivel de Riesgo Inherente y como producto de la aplicación de controles establecer el nivel de Riesgo Residual.

Ilustración 11. Riesgo residual.



Fuente: Elaboración propia OAP

8.9.1. Diseño de controles

Los controles se pueden formular por medio de varios mecanismos, bien sea a través de las entrevistas con los líderes de procesos o los enlaces MIPG o los servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos, formatos que el proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo. Se recomienda que los controles a incluir en las matrices de riesgos se encuentren dentro de algún documento del sistema de gestión de la entidad.
Las actividades de control deben atender las causas raíz y enfocarse en la gestión de los factores de riesgo. Para ser efectivas deben contar con todos los atributos descritos en el presente numeral y cuando estén directamente relacionadas con las causas y factores de riesgo.

Para determinar la efectividad del control se debe tener en cuenta:

a. Estructura para la descripción del control

Responsable: Determina el cargo del responsable que ejecuta el control, se debe considerar la denominación del rol (Director, asesor, profesional, técnico, asistencial, profesional contratista

designado). Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.

Se debe considerar que el responsable definido cuenta con el nivel de autoridad apropiado de cara a la actividad de control, así como aspectos básicos de segregación de funciones para evitar que quién sea la fuente generadora de riesgo, sea el único que aplica alguna actividad de control.

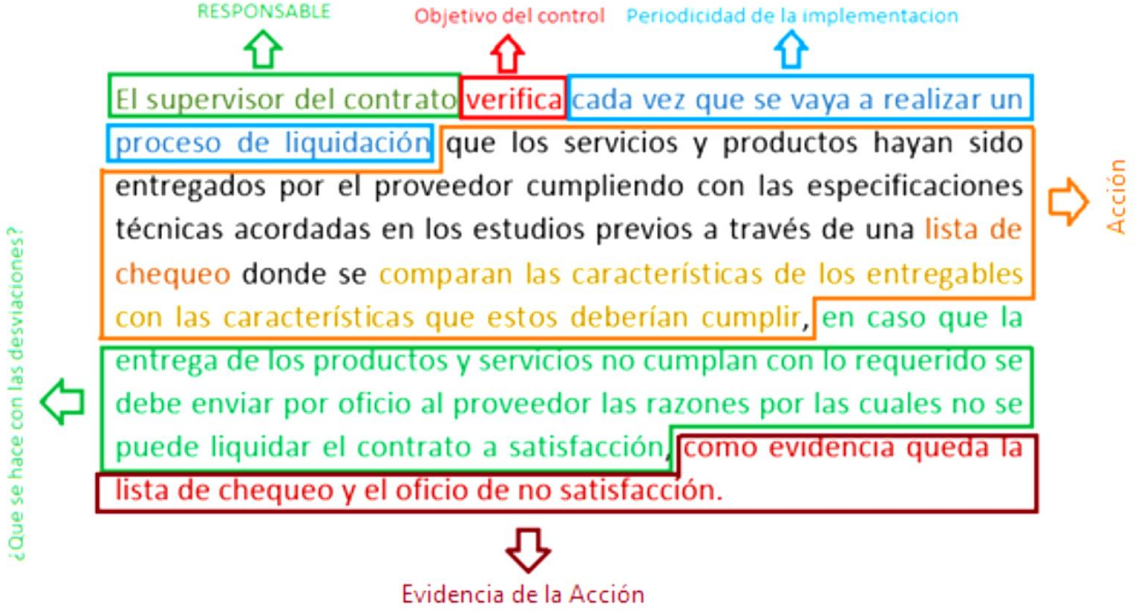
Objetivo del control: Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control. Ejemplos (Verificar, validar, conciliar, comparar, revisar, cotejar, detectar)

Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control.

- Frecuencia (periodicidad de la implementación): Corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para prevenir, detectar o corregir el posible evento de riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
- Ejecución (Acción): Permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de presentarse desviaciones o situaciones que impidan su desarrollo. Puede darse a través de la comparación con información interna, externa o mixta. Se recomienda que su definición esté registrada en el sistema de gestión de la entidad (procedimientos, guías, instructivos, manuales, políticas, etc.).
- Evidencia documentada (evidencia de la acción): Se refiere a la fuente documental que permite evidenciar la ejecución de los controles, bien sea formatos, base de datos, lista de chequeo, un acta de reunión, etc. Puede ser registro físico, manual o electrónico.

La siguiente es la estructura del control recomendada:

Ilustración 12. Estructura del control.



Fuente: Elaboración propia JB-JCM

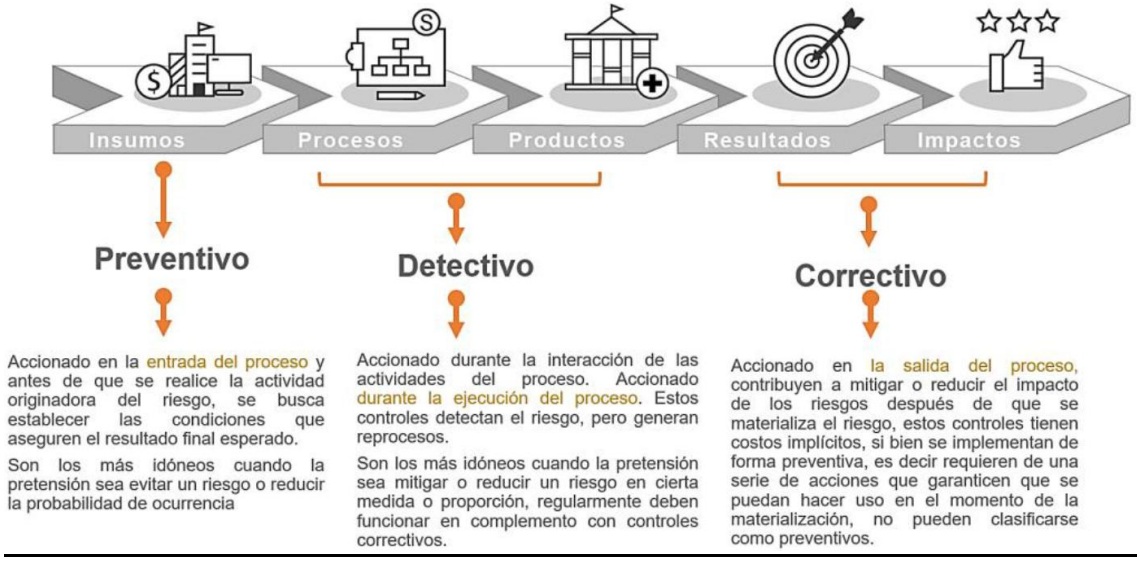
Tipología de controles

Control Preventivo: Control accionado en la entrada del proceso y antes que se realice la actividad originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado

Control Detectivo: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo, pero generar reprocesos.

Control Correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Ejemplos: pólizas de seguro, copias de seguridad (backup), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializado.

Ilustración 13. Tipologías de control.



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

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

- Control manual: ejecutados por personas.
- Control automático: ejecutados por un sistema o software previamente programado o diseñado.

b. Análisis y evaluación de los controles

Teniendo en cuenta las características propias del control se realiza su evaluación, a través de estos atributos:

Tabla 8. Atributos del control.

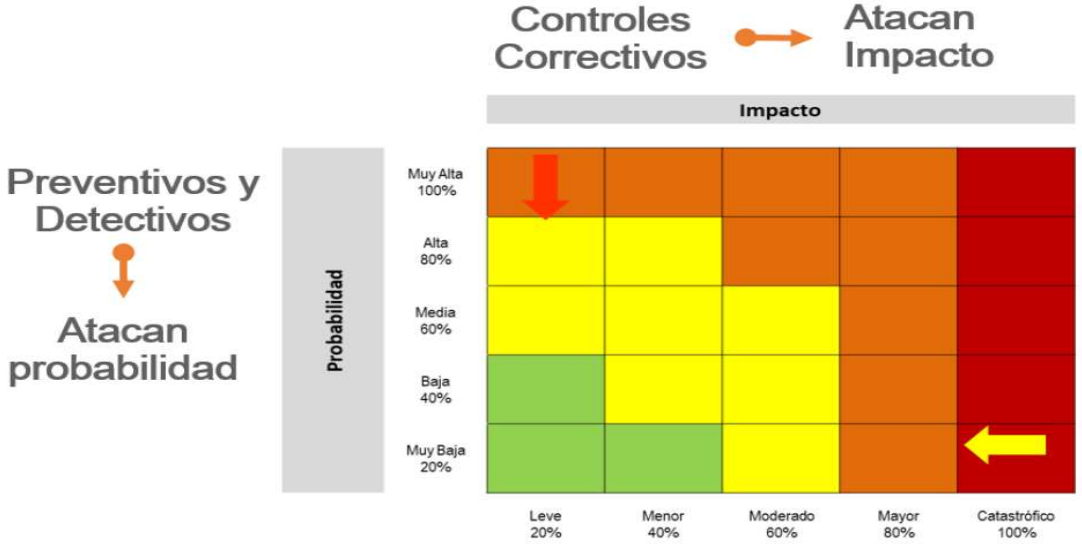
Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten 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 Informativos	Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.	-
		Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).	
		Otros Esquemas	Políticas de operación, manuales o guías específicas.	-
	Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.	-
		Periódicamente (diario, mensual, bimestral, trimestral, semestral).		-
	Evidencia	Con registro manual	Se deja evidencia o rastro de la ejecución del control.	-
		Con registro electrónico		-
	Ejecución	Interna	Formatos o registros internos formales.	=
		Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).	=
		Mixta	Combinación de datos de fuentes internas y externas formales.	=

Fuente: Fuente: Elaboración propia JB-JCM

8.10. Aplicación de controles y Riesgo residual

A partir de la aplicación de controles se obtiene el movimiento o desplazamiento del nivel de riesgo inherente 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.

Ilustración 14. Desplazamiento Mapa de calor.



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

El Riesgo Residual corresponde al estado real del riesgo, luego de la valoración del riesgo inherente y la aplicación de los controles; lo que conlleva a identificar la necesidad de implementación de controles o mejoras adicionales sobre los existentes.

La fórmula dada para valorar los controles que afecten la probabilidad equivale a la resta de la valoración dada a la probabilidad de ocurrencia del riesgo menos el resultado de multiplicar la valoración dada a la probabilidad de ocurrencia del riesgo por el valor del control.

PI= Probabilidad Inherente
PR= Probabilidad Residual
VC= Valoración del Control

PR = PI – (PI * VC)

Como puede existir más de un control para mitigar la misma probabilidad de ocurrencia de un riesgo, para el segundo control se tomará PR como PI.

PR1 = PI – (PI * VC1)
PR2 = PR1 – (PR1 * VC2)
PR3 = PR2 – (PR2 * VC3)
PRn = PRn-1 – (PRn-1 * VCn)

Lo mismo ocurre para la valoración de los controles que afecten el impacto siendo la fórmula resultante la que se muestra a continuación:

II= Probabilidad Inherente
IR= Probabilidad Residual
VC= Valoración del Control

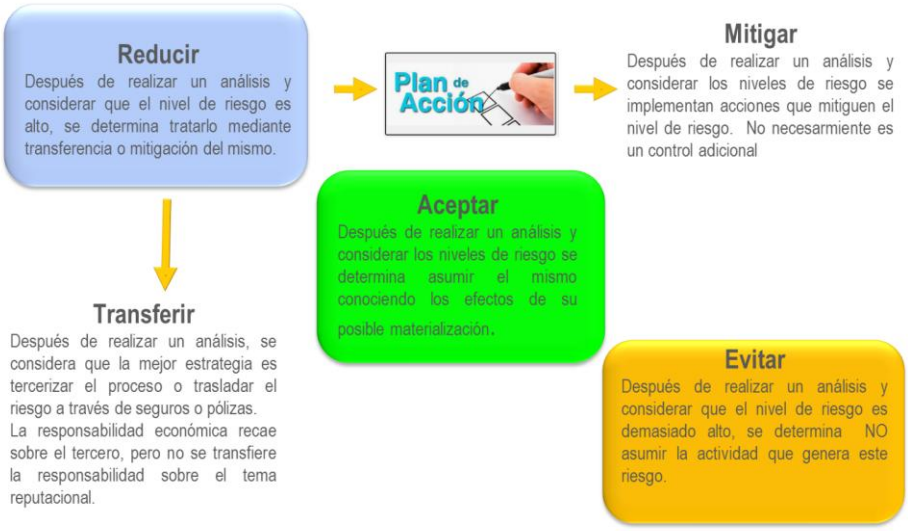
IR1 = II – (II * VC1)

IR2 = IR1 – (IR1 * VC2)
IR3 = IR2 – (IR2 * VC3)
IRn = IRn-1 – (IRn-1 * VCn)

8.11. Tratamiento del Riesgo

Esta etapa se busca establecer las acciones que se aplicarán a los riesgos identificados luego de la obtención del riesgo residual considerando aplicar las opciones de tratamiento de acuerdo con el nivel de riesgo obtenido y desarrollar planes en caso de ser necesario.
A continuación, se describen las opciones para el tratamiento del riesgo:

Ilustración 15. Tratamiento del Riesgo.



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

- Reducir: luego de los resultados obtenidos se determina mediante transferencia o mitigación, en ambos casos corresponde a la Implementar controles para reducir la probabilidad o el impacto.
  - Transferir: Compartir las consecuencias de la materialización del riesgo, por ejemplo, a través de la adquisición de una póliza.
  - Mitigar: Acciones adicionales que mitiguen el nivel de riesgo.
- Aceptar: Cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección.
- Evitar: Cuando se decide evitar la realización de la actividad que representa el riesgo.

Verificar para cada tipología de riesgo el tratamiento en el desarrollo de su capítulo.

8.12. Consolidación en el mapa de riesgos.

Los resultados obtenidos en el desarrollo de los anteriores numerales se consolidan en la matriz de riesgos institucional evidenciando lo desarrollado para cada una de las tipologías de riesgos que se gestionan en la entidad.

9. TIPOLOGÍAS DE RIESGO

La entidad asume la gestión integral de riesgos y mediante la presente política gestiona las siguientes tipologías: Gestión, Fiscal, Seguridad de la Información e Integridad pública.

Sin embargo, el presente lineamiento permite la articulación y vinculación con las Políticas y entornos de seguimiento establecidos para el ejercicio e implementación del Modelo Integrado de Planeación y Gestión - MIPG.

9.1. Riesgos de Gestión.

Corresponde a los riesgos asociados a la operación de la entidad, al ser propios o intrínsecos a los procesos, funciones y misionalidad de cada entidad. Los riesgos de gestión son aquellos posibles efectos que se causan sobre los objetivos de la entidad, debido a eventos potenciales, que hacen referencia a la posibilidad de incurrir en pérdidas económicas o reputacionales por deficiencias, fallas o inadecuaciones, en la “ejecución y administración de procesos”,” tecnología” e “infraestructura”, generados por falencias en la operación.

Por lo anterior la selección de los siguientes factores determina la clasificación del evento de riesgo en la tipología de Gestión:

Tabla 9. Factores de riesgos de Gestión.

Factor	Definición	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos
		Falta segregación de funciones
		Errores de grabación, autorización
		Falta de supervisión o interventoría
		Errores en cálculos para pagos internos y externos
		Alta rotación o insuficiencia de personal
		Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
		Acciones contrarias a las leyes o acuerdos contractuales
		Falta de capacitación y otros temas relacionados con el personal
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Hurto activos
		Caída de sistemas de información y aplicaciones
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Para esta tipología de riesgos se desarrollan los siguientes numerales sin modificación:

8.8. Estructura de la descripción del Riesgo
8.9. Diseño, Análisis y Valoración de Controles
8.10. Aplicación de controles y Riesgo residual
8.11. Tratamiento del Riesgo
8.12. Consolidación en el Mapa de Riesgos

9.2. Riesgos de Seguridad de la Información.

Los lineamientos para la formulación e implementación de la Gestión de Riesgos de Seguridad de la Información que se puedan presentar en el desarrollo de la gestión de la entidad y están fundamentados en el Anexo 4. “Lineamientos para la Gestión de Riesgos de Seguridad Digital en entidades públicas” del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, ISO/IEC 27002:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad — Controles de seguridad de la información y la “Guía para la Gestión Integral del Riesgo en Entidades Públicas” del Departamento Administrativo de la Función Pública - DAFP.

Los Riesgos de Seguridad Digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, Confidencialidad o Disponibilidad” que permiten cumplir con la misión y alcanzar la Visión de la entidad.

- **Integridad:** Se refiere a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros no autorizados.
- **Confidencialidad:** Se refiere a cómo los datos se mantienen al acceso únicamente de las personas o sistemas que se encuentran autorizados.
- **Disponibilidad**: Se refiere al acceso de la información en el momento que debe estar disponible; se aclara que la información de la entidad no debe estar disponible todo el tiempo durante el año.

En tal sentido, para la identificación de Riesgos de Seguridad de la Información es necesario en primera instancia identificar los activos de información de la entidad y los procesos, teniendo en cuenta los siguientes pasos:

9.2.1. Identificación de los activos de seguridad de la información.

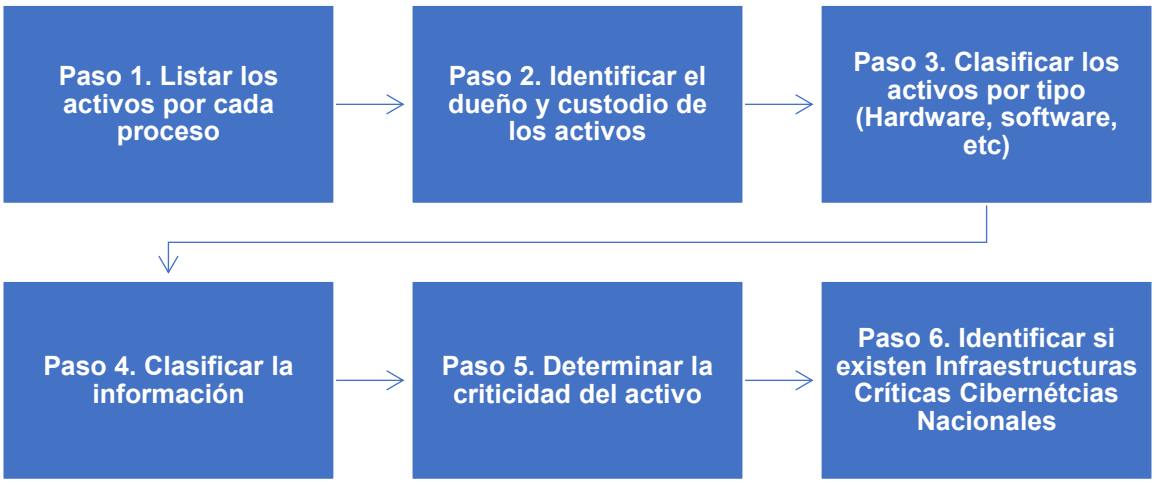
Para la Identificación de Riesgos de Seguridad de la Información es necesario contar con el inventario de activos de información por proceso aprobado y publicado. Es importante recordar que un activo de información es cualquier información que aporte valor a la entidad dentro de los cuales se pueden encontrar elementos (información, aplicaciones, hardware, personas, entre otros), que se deben proteger para garantizar el funcionamiento interno de cada proceso.

Los líderes de los procesos del JBJCM deben coordinar las actividades necesarias para realizar el levantamiento, actualización y clasificación de los activos de la información con el acompañamiento de la Oficina Asesora de Planeación representado en el apoyo del Oficial de Seguridad y Privacidad de la Información. De igual forma para la Gestión de los Riesgos de Seguridad Digital, los líderes de cada proceso deben definir los activos de información, clasificarlos e identificar si existen infraestructuras criticas cibernéticas, teniendo en cuenta las situaciones no deseadas, la pérdida de confidencialidad, integridad y disponibilidad de la información, así poder identificar los activos que requieren ser

custodiados y protegidos que permitan garantizar el funcionamiento interno en el JBJCM, así como el funcionamiento de cara al ciudadano.

Los siguientes son los pasos para desarrollar para la identificación y valoración de activos.

Ilustración 16. Pasos para la identificación y valoración de activos



Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

9.2.2. Identificación de Riesgos de Seguridad de la información.

La Gestión de los Riesgos de Seguridad Digital y Privacidad de la Información se ejerce en integración con el MSPI (Modelo de Seguridad y Privacidad de la Información) y con el MGRSD (Modelo de Gestión de Riesgos de Seguridad de la Información) determinado por MINTIC. Así mismo, en la determinación de las fases para la Gestión de Riesgos, se incluyen las ICC (Infraestructuras Críticas Cibernéticas) como parte de los activos de la información del JBJCM.

Las afectaciones que pueden generar daño a un activo o un grupo de activos inherentes a la seguridad de la información son:

- Pérdida de confidencialidad de la información.
- Pérdida de la integridad de la información.
- Pérdida de la disponibilidad de la información.

Dentro de las amenazas podemos identificar amenazas comunes como son, aquellas que causan daño a la infraestructura tecnológica, a los servicios, al cumplimiento de las funciones y comprometiendo así los activos. Pueden ser Deliberadas (D), fortuitas (F) o ambientales (A). la siguiente es la relación de amenazas comunes:

Tabla 10. Tabla de amenazas comunes.

Tipo	*Amenaza*	*Origen*
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A

Tipo	*Amenaza*	*Origen*
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Del mismo modo se cuenta con la relación de las vulnerabilidades comunes:

Tabla 11. Tabla de Vulnerabilidades Comunes.

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

El desarrollo de la metodología se efectúa en el documento “Gestión de Riesgos de Seguridad de la Información – Digital” para identificar, analizar, valorar, evaluar y tratar los Riesgos de Seguridad Digital, a fin de contribuir al cumplimiento de los requisitos de la entidad, propendiendo el cumplimiento de sus objetivos estratégicos, requisitos legales y reglamentarios, visión y misión, conservación de la confidencialidad, integridad y disponibilidad de la información.

Para la valoración de los controles se tendrá en cuenta los controles de la norma estándar “ISO/IEC 27002:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad — Controles de Seguridad de la Información”, así mismo el diseño varía en relación con el identificador, nombre y propósito de cada control y se refleja en Mapa de Riesgos Sistema Seguridad de la Información-Digital para su tratamiento por proceso. En el Manual Gestión de Riesgos de Seguridad de la Información – Digital SDI.PR.02. M.01 se podrá evidenciar a detalle la gestión antes informada.

Para esta tipología de riesgos se desarrollan los siguientes numerales sin modificación:

8.8. Estructura de la descripción del Riesgo
8.9. Diseño, Análisis y Valoración de Controles
8.10. Aplicación de controles y Riesgo residual
8.11. Tratamiento del Riesgo

9.2.3. Consolidación en el Mapa de Riesgos

Dada su especificidad y tratamiento los riesgos de Seguridad de la información se consolidan individualmente en la matriz de riesgos de seguridad de la información.

9.3. Riesgos Fiscales

Corresponde al análisis de la operación de la entidad para identificar y gestionar los riesgos que puedan provocar un daño patrimonial, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del estado.

Las bases del ámbito normativo y jurídico del control fiscales están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, modificadas por el Acto Legislativo 04 de 2019 fundamentado en la necesidad de un ejercicio preventivo del control fiscal, que detenga el daño fiscal e identifique los riesgos fiscales en la entidad; con ello, la línea estratégica podrá adoptar las medidas necesarias para prevenir la concreción del daño patrimonial de naturaleza pública.

El Riesgo Fiscal se define como el “Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial”, el cual surge de los daños que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, si bien La Ley 610 de 2000 establece el trámite de los procesos de responsabilidad fiscal es de competencia de las contralorías, se evidencia que el control fiscal efectuado por dichas entidades además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante con carácter excepcional, no vinculante, no implica coadministración, no versa sobre la conveniencia de las decisiones de los administradores de recursos públicos, se realiza en forma de advertencia al gestor fiscal y deberá estar incluido en un sistema general de advertencia público; se busca generar el desarrollo preventivo al interior de la entidad con el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, protegiendo la

entidad de la perdida de recursos públicos, bienes o intereses patrimoniales a cargo de los gestores fiscales (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros), lo cual contribuye al cumplimiento de sus funciones y al aseguramiento razonable para la toma de decisiones.

9.3.1. Identificación de áreas de factores de riesgo

Las fuentes generadoras de riesgos para esta tipología aplican todos los factores relacionados en la tabla 4 debido a que todas las circunstancias o condiciones pueden aumentar la probabilidad de que ocurra el evento de riesgo fiscal.

9.3.2. Identificación del Riesgo

Para la identificación del Riesgo Fiscal es necesario seguir los siguientes pasos:

Ilustración 17. Pasos para la identificación del riesgo fiscal

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Para establecer los **puntos de Riesgo Fiscal** que corresponde a las actividades 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, se toman como punto de partida aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal en la entidad.

Complementando el ejercicio de los puntos de riesgo se deben identificar las **circunstancias inmediatas**, siendo aquellas situaciones o actividades bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o causa raíz para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas. Para mantener unificado el criterio de identificación del riesgo la **Circunstancia Inmediata** corresponde a la **Causa Inmediata** definida para los Riesgos de Gestión.

9.3.3. Identificación de Puntos de Riesgo Fiscales y Causa Inmediata

Como complemento a la identificación del riesgo se debe adelantar el siguiente cuestionario:

- **Cuestionario de Identificación:** Se debe efectuar con los líderes de procesos u operativos, en compañía de los asesores y servidores que se consideren necesarios 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 causas inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal).

    - ¿En qué procesos de la entidad se realiza Gestión Fiscal?
    - ¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo 1), son aplicables a la entidad?
    - ¿Cuáles son los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal relacionados con hechos de la entidad y las advertencias recibidas por Contraloría de Bogotá o la OCI?
    - ¿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?

Los ejercicios antes descritos deben efectuarse como mínimo una vez al año y deben respaldarse con actas de reunión con los líderes de proceso u operativos. El ejercicio se respalda con la verificación de Matriz de Plan de Mejoramiento de Contraloría de la entidad y la asesoría de la OCI.

9.3.4. Identificación de áreas de impacto

Para el contexto del 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 esta tipología de riesgo.

Para definir el área de impacto, al momento de identificar y redactar riesgos fiscales, es fundamental tener claro el concepto de patrimonio público a partir de las tres expresiones que se derivan del artículo 6 de la Ley 610 de 2000:

Tabla 12. Pasos para la identificación del riesgo fiscal

Bienes públicos: Son todos aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público (aquellos cuyo uso pertenece a todos los habitantes del territorio nacional) y bienes fiscales (aquellos que están destinados al cumplimiento de las funciones o servicios públicos).
Recursos públicos: Son los dineros comprometidos y ejecutados en ejercicio de la función pública.
Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

9.3.5. Identificar el efecto económico

Es importante precisar que el efecto económico del riesgo fiscal es determinado como el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público. De la misma manera es importante indicar 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.

Lo siguientes son ejemplos de efectos económicos que no son riesgos fiscales:
(i) Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
(ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, 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
(iii) Multas impuestas por hechos que no comportan gestión fiscal
(iv) Existencia de actuación de cobro coactivo por parte de la entidad.
(v) Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.
(vi) Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su “normal uso” (máquinas eléctricas, computadores, celulares, etc.). (Contraloría General de la República, 2023, p. 12).

9.3.6. Identificación de la causa raíz o potencial hecho generador

La causa raíz o potencial hecho generador es aquel evento potencial (acción u omisión) que 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/Impacto) 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.

Para mantener la adecuada Gestión del Riesgo se exige que la identificación de causas sea objetiva y rigurosa, permitiendo ya que los controles que se diseñen e implementen apunten a atacar las causas, para así lograr prevenir la ocurrencia de daños fiscales.

9.3.7. Descripción del Riesgo Fiscal

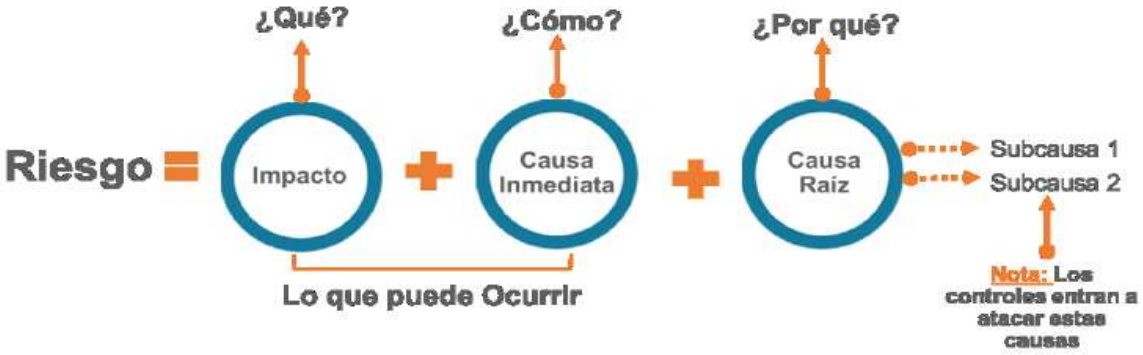
Para lograr diferenciar los riesgos fiscales de las demás tipologías se debe formular y redactar adecuadamente permitiendo su entendimiento y tratamiento pertinente.

Para redactar un Riesgo Fiscal se debe tener en cuenta:
✓ Iniciar con la expresión **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

✓ Causa (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.
✓ 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:

Ilustración 18. Estructura del riesgo.



Fuente: Elaboración propia.

La descripción del riesgo debe contener todos los detalles antes ilustrados con la intención de que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. La estructura facilita su redacción y claridad, evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

A continuación, la estructura de redacción de un riesgo fiscal dando atención a lo manifestado:

Ilustración 19. Estructura del Riesgo Fiscal.

Fuente: Elaboración Propia

Otros ejemplos de Riesgos Fiscales son:

Tabla 13. Ejemplos de Riesgo Fiscal.

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 implementación y operación de redes eléctricas seguras.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por negación del reconocimiento de siniestros en el contrato de seguro, a causa de la omisión en la actualización del inventario de bienes amparados.
Posibilidad de efecto dañoso sobre bienes públicos, por pérdida, extravío o hurto de bienes muebles de la entidad a causa de la inexistencia de procedimientos documentados para el ingreso y salida de bienes del almacén	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 menores ingresos percibidos sobre la explotación de marcas de propiedad comercial de la entidad a causa de errores u omisiones en el análisis técnico, jurídico y económico del mercado
Posibilidad de efecto dañoso sobre bienes públicos, por deterioro de la infraestructura a causa de la realización de la programación de mantenimientos preventivos y correctivos	Posibilidad de efecto dañoso sobre los recursos de la entidad por la generación de intereses moratorios en contrato de arrendamiento a causa de la omisión en el pago oportuno del canon pactado.	Posibilidad de efecto dañoso sobre los intereses patrimoniales por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Para esta tipología de riesgos se desarrollan los siguientes numerales sin modificación:

8.8. Estructura de la descripción del Riesgo (A partir del numeral 8.8.1)
8.9. Diseño, Análisis y Valoración de Controles
8.10. Aplicación de controles y Riesgo residual
8.11. Tratamiento del Riesgo
8.12. Consolidación en el Mapa de Riesgos

9.4. Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP

Con la expedición de la Ley 2195 de 2022, que hace obligatorio para el JBJCM la “prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional” (artículo 31), por lo anterior la Secretaría de Transparencia de la Presidencia de la República sugiere que el Programa de

Transparencia y Ética Pública – PTEP cuente con un sistema de gestión que permita prevenir, detectar y corregir los eventos que amenacen el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), para esto se ha adoptado el Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, que se desarrolla a continuación.

En todo caso, de acuerdo con el parágrafo 1 del artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, la Política para la Gestión Integral de Riesgos, se articula con el PTEP y, en consecuencia, con el SIGRIP.

Teniendo en cuenta las diferentes amenazas para la integridad pública manifestadas en el presente numeral, que pueden generar peligro o daño, es necesario que, desde un enfoque basado en riesgos, se gestionen los eventos que pueden ocurrir en la entidad, mediante la identificación, análisis y valoración de posibles eventos de riesgo asociados.

Es importante manifestar que un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causa el soborno, el fraude, un conflicto de intereses gestionado inadecuadamente o la corrupción. Además, puede también favorecer el lavado de activos, la financiación del terrorismo o la financiación de la proliferación de armas de destrucción masiva. Por esta razón, es necesario abordar los riesgos para la integridad pública de forma integral y en estrecha articulación con las demás tipologías de riesgos.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP contempla que la entidad actúe con diligencia en el conocimiento de sus contrapartes y que integre el equipo de cumplimiento, sumado a lo establecido en la presente Política para la Gestión Integral de Riesgos.
A continuación, desarrollamos cada uno de los términos que componen el SIGRIP:

9.4.1. Integridad pública

En el entendido que el JBJCM como entidad pública se expone a que sus objetivos no se cumplan como consecuencia de diferentes intereses que pueden confluir en la toma de decisiones, en la medida que se puedan privilegiar intereses propios sobre el interés general de la organización, lo que termina afectando la capacidad de la entidad para cumplir con las funciones que se le han encomendado.
En materia de integridad para la entidad, se espera que los servidores, y en general los colaboradores, dentro de un marco ético, se comporten de forma que privilegien el interés general del JBJCM en todas las decisiones que deben tomar en el ejercicio de sus funciones o del servicio que prestan. Si bien los servidores tienen diferentes normas que establecen ese comportamiento deseado y una máxima en materia de responsabilidad, es importante recalcar que son responsables tanto de sus acciones como de sus omisiones, tal como lo establece la Constitución Política Colombiana. Manifestado lo anterior, cualquier decisión que no privilegie la entidad es un incumplimiento de la conducta deseable que constituye una actuación que pone en riesgo a la integridad.

En suma, la entidad asegura que exista y se promulgue una cultura de cumplimiento institucional, partiendo del reconocimiento del individuo y su propia ética, para asegurar que éste actúe de forma íntegra, que no es otra cosa distinta que actuar con apego a la ley. Adicional a la cultura de cumplimiento que promociona la legalidad, garantizando la integridad, se adoptan medidas para gestionar todas las posibles incertidumbres que pueden poner en riesgo la garantía del interés general.

9.4.2. Amenazas para la integridad pública.

La Organización para la Cooperación y el Desarrollo Económico - ODCE, plantea la necesidad de aplicar un enfoque basado en riesgos cuando se habla de integridad pública. Manifiesta las amenazas que pueden incidir en diferentes puntos de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en particular, asegurar el cumplimiento de la ley. El JBJCM se centra en las cinco amenazas para la integridad recomendadas por dicha organización y promovidas por Función Pública:

9.4.2.1. Soborno

Entendido como “ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]”. El soborno opera en dos entornos: Entrante y Saliente. El soborno Entrante corresponde al soborno suministrado al servidor de la Entidad, y Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

En el Código Penal Colombiano está tipificado como cohecho propio, cohecho impropio, cohecho por dar u ofrecer, todos delitos contra la administración pública, que son formas de soborno. Solamente entre particulares tipifica de forma general el soborno.

9.4.2.2. Fraude

Corresponde a errores, omisiones, reportes/informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima.

El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

9.4.2.3. Conflicto de intereses

Surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entra en conflicto con un interés particular y directo del servidor público.

Si bien la sola existencia del conflicto de intereses no implica una conducta reprochable, sí existen una serie de comportamientos definidos por códigos de conducta sobre la declaración y gestión del conflicto de intereses. La legislación nacional estima que quien tenga un interés particular en un asunto público está impedido para tomar la decisión.

9.4.2.4. Corrupción

Es *"todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral"*[2].

9.4.2.5. Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) - LA/FT/FP

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva – LA/FT/FP. A través de estas prácticas y conductas se compromete la capacidad de la entidad para cumplir con sus fines, en la medida que puede ser usada para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando la institución.

9.4.3. Operación del SIGRIP

Para que el SIGRIP pueda operar adecuadamente, el JBJCM dispone de lo siguiente:

- El recurso financiero, tecnológico y humano para el funcionamiento de la Presente Política, el PTEP y la función de cumplimiento que en la entidad es asumida por el equipo de cumplimiento.

- El recurso humano relacionado con el funcionamiento del SIGRIP, el equipo de cumplimiento, el PTEP y la presente Política debe corresponder a profesionales universitarios con experiencia en la Gestión de riesgos mínimo de 6 meses.

- El desarrollo de dos (2) sensibilizaciones al año que permitan asegurar la toma de conciencia del personal, los líderes, el administrador, la Alta Dirección y, en general, de toda la organización, sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP. A su vez incluir dentro de la acción de Formación del Programa de Transparencia y Ética Pública la toma de conciencia sobre:

    - Los objetivos y alcance del Sistema
    - Cada uno se sus elementos.
    - Los beneficios que tiene el Sistema para la organización.
    - Las implicaciones del incumplimiento de los requisitos del Sistema

- Publicación en la página web de la entidad del informe del SIGRIP, los resultados de su operación, así como cualquier actualización del Sistema o de algunos de sus elementos. A su vez incluir dentro de la acción de Comunicación del Programa de Transparencia y Ética Pública:

[2] artículo 2.1.4.3.1.3 del Decreto 1081 de 2015

Los lineamientos sobre la forma en que se comunicará, su periodicidad, los resultados del Sistema, así como cualquier actualización que se introduzca.

- Promoción de la Gestión archivística de la entidad y del sistema de gestión con los elementos necesarios para el funcionamiento del SIGRIP, permitiendo asegurar la protección de los datos personales y la confidencialidad, en el caso de la información clasificada o reservada. En cada elemento del sistema, deberá evaluarse individualmente el tratamiento que debe darse a la información documentada.

Para gestionar completamente los riesgos asociados a soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción y LA/FT/FP, se requiere de tres elementos adicionales que son fundamentales para el SIGRIP: la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas de gestión del riesgo.

La estructura del SIGRIP se detalla a continuación:

Ilustración 20. Estructura del SIGRIP

Fuente: Guía para la Gestión integral del Riesgo en Entidades Públicas (V7) – DAFP

Las amenazas ya se han manifestado previamente en la presente Política, respecto a la (i) debida diligencia en el conocimiento de las contrapartes, que es efectuada a través de lo designado por el (ii) equipo de cumplimiento (función de cumplimiento) y (iii) las herramientas fortalecen la aplicación del SIGRIP, se desarrollan en la Política SARLAFT, lineamiento que complementa el desarrollo del sistema y el presente lineamiento.

9.4.4. Identificación de riesgos.

Sumado a lo descrito en el numeral "**8.5.** Identificación de riesgos", es importante manifestar que en el marco de los eventos asociados a LA/FT/FP, los puntos de riesgo se refieren a operaciones que lleva a cabo la entidad. Es decir, actividades dentro del flujo de los procesos que implican un intercambio de recursos, bien sea porque la entidad recibe un bien o servicio por el cual paga un precio, o porque entrega un bien o servicio por el cual le pagan un precio. Estas operaciones son los puntos de riesgo, que deben tenerse en cuenta para la identificación del riesgo de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

Respecto del riesgo de Corrupción y sus manifestaciones específicas como soborno, fraude e inadecuada gestión del conflicto de intereses, los puntos de riesgos pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones, lo anterior debido a que son ejecutadas por personas, siendo esta la fuente de su posible exposición.

9.4.5. Identificación de áreas de impacto

Además del impacto económico y reputacional, para los riesgos de Integridad pública también puede haber consecuencias legales y de contagio.

La consecuencia legal corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños. Por lo tanto, el impacto legal surge desde el momento en que una contraparte es vinculada a procesos judiciales o administrativos sancionatorios o que busquen declarar un incumplimiento.

El contagio corresponde a la posibilidad de que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una contraparte. El contagio se expresa cuando a contrapartes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad.

Las consecuencias legales y de contagio, para efectos de determinar el impacto del riesgo, deben analizarse en términos de afectación económica, atendiendo a lo indicado en el numeral **8.1** de la presente Política.

9.4.6. Identificación de áreas de factores de impacto.

Los siguientes son los factores que intervienen para los riesgos de integridad pública:

Tabla 14, Factores de riesgo integridad pública.

Factor	Definición	Descriptores
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas)
		Productos (bienes o servicios) que oferta/requiere
		Canales utilizados para la operación
		Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Fraude Interno
		Soborno entrante
		Soborno saliente
		Gestión inadecuada de conflicto de Intereses
		Corrupción

Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

Como factores del riesgo LA/FT/FP se tiene a las contrapartes, los productos, los canales y las jurisdicciones, los cuales en conjunto conforman el concepto de “transacción” u “operación”, en el entendido que una transacción, en todos los casos, será realizada por un cliente o usuario, que accedió o entregó un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica. Estos factores deben permitirle a la entidad mayor efectividad en el conocimiento de las

contrapartes, el diseño y aplicación de señales de alerta, la identificación de operaciones inusuales y la determinación y el reporte de operaciones sospechosas.

9.4.7. Estructura de la Descripción del riesgo.

La descripción de los riesgos para la integridad pública mantiene la estructura definida para las demás tipologías del riesgo descrita en la **ilustración 6**. Todos inician con la formula “Posibilidad de”, seguido del impacto, la causa inmediata y la causa raíz.

Teniendo en cuenta las amenazas descritas las causas inmediatas de los riesgos para la integridad pública son el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.

Tabla 15, Estructura del riesgo de integridad pública.

Impacto	Causa inmediata	Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	
	Soborno Saliente	
	Gestión inadecuada de Conflicto de interés	
	Corrupción	
Económico, Reputacional, Legal, Operativo o de Contagio	LA/FT/FP	Descripción de la Operación o Transacción

Fuente. Guía para la Gestión Integral del Riesgo en entidades Públicas. Versión 7. DAFP. 2025

A continuación, algunos ejemplos de riesgos de integridad pública:

- Posibilidad de afectación económica por Corrupción en la evaluación en la evaluación de los procesos de selección para la contratación de bienes y servicios de la Entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico
- Posibilidad de afectación económica por Fraude Interno en la asignación de subsidios a causa de errores, omisiones, informes inexactos o descripciones incorrectas realizados para beneficio personal o de terceros en la asignación de subsidios.
- Posibilidad de afectación reputacional por Soborno Saliente en el seguimiento a la agenda legislativa de la Entidad, a causa del ofrecimiento indebido de incentivos o recompensas para que una persona actúe o se abstenga de actuar en favor de la entidad.
- Posibilidad de afectación reputacional por Soborno Entrante al aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.
- Posibilidad de afectación económica por conflicto de interés no declarado y/o declarado, pero no gestionado y/o declarado y no aceptado, a causa de decisiones en asuntos sobre los cuales la servidora o servidor público tiene un interés particular en desarrollo del comité de contratación.
- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas en las operaciones de pago de subsidios.
- Posibilidad de contagio por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades

terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de contratación directa.

- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de recaudo.

Para esta tipología de riesgos se desarrollan los siguientes numerales sin modificación:

8.8. Estructura de la descripción del Riesgo (8.8.1 en adelante)
8.9. Diseño, Análisis y Valoración de Controles
8.10. Aplicación de controles y Riesgo residual
8.11. Tratamiento del Riesgo
8.12. Consolidación en el Mapa de Riesgos

10. MONITOREO, SEGUIMIENTO Y EVALUACIÓN DE LOS MAPAS DE RIESGOS

La aplicación de la presente política, así como la implementación del SIGRIP se efectuará bajo el siguiente esquema:

Tabla 16. Reporte de mapas de Riesgo.

LINEA DE DEFENSA	GESTIÓN/FISCALES	SEGURIDAD DE LA INFORMACIÓN	INTEGRIDAD PÚBLICA
PRIMERA (Líder del Proceso)	Realiza el reporte del avance de la implementación de los controles y de las acciones formuladas en el Portal MIPG, junto a las evidencias de ejecución para su tratamiento en el repositorio administrado por la OAP, cada cuatro (4) meses, es decir, con corte a 30 de abril, 31 de agosto y 31 de diciembre, en los cinco (5) primeros días hábiles al corte a la Oficina Asesora de Planeación, como segunda línea de defensa.	Realiza el reporte del avance de la implementación de los controles y de las acciones formuladas en el mapa de riesgos junto a las evidencias de ejecución para su tratamiento cada cuatro (4) meses, es decir, con corte a 30 de abril, 31 de agosto y 31 de diciembre, en los diez (10) primeros días hábiles al corte a la Oficina Asesora de Planeación, como segunda línea de defensa.	Realiza el reporte del avance de la implementación de los controles y de las acciones formuladas en el Portal MIPG, junto a las evidencias de ejecución para su tratamiento en el repositorio administrado por la OAP, cada cuatro (4) meses, es decir, con corte a 30 de abril, 31 de agosto y 31 de diciembre, en los cinco (5) primeros días hábiles a la Oficina Asesora de Planeación, como segunda línea de defensa.
SEGUNDA (Oficina Asesora de Planeación)	Realiza alertamiento del incumplimiento de los procesos que no reportaron oportunamente o con inconsistencias, en los diez (10) primeros días hábiles al corte, a través de correo electrónico. Hace seguimiento y retroalimenta a los procesos	Realiza alertamiento del incumplimiento de los procesos que no reportaron oportunamente o con inconsistencias, en los diez (10) primeros días hábiles al corte, a través de correo electrónico. Hace seguimiento y retroalimenta a los procesos	Realiza alertamiento del incumplimiento a los procesos que no reportaron oportunamente o con inconsistencias, el cinco (5) día hábil de los meses de corte, a través de correo electrónico. Hace seguimiento y retroalimenta a los procesos

LINEA DE DEFENSA	GESTIÓN/FISCALES	SEGURIDAD DE LA INFORMACIÓN	INTEGRIDAD PÚBLICA
	en el avance de la implementación de los controles y de las acciones formuladas, cada cuatro (4) meses, a través del informe de seguimiento y matriz de riesgos, en los diez (10) primeros días hábiles al corte del reporte. Reporta el resultado del seguimiento a la OCI, a través del informe de seguimiento y la Matriz de Riesgos Institucional en los quince (15) primeros días hábiles al corte. Publica el informe de seguimiento y la Matriz de Riesgos Institucional en la carpeta Unidad MIPG y la web de la Entidad, en los quince (15) primeros días hábiles al corte.	en el avance de la implementación de los controles y de las acciones formuladas, cada cuatro (4) meses, a través del informe de seguimiento y matriz de riesgos, en los quince (15) primeros días hábiles al corte del reporte. Reporta el resultado del seguimiento a la OCI, a través del informe de seguimiento y la Matriz de Riesgos Institucional en los veinte (20) primeros días hábiles al corte. Publica el informe de seguimiento y la Matriz de Riesgos Institucional en la carpeta Unidad MIPG o en Repositorio "Seguridad Digital" en los veinte (20) primeros días hábiles al corte. *	en el avance de la implementación de los controles y de las acciones formuladas, cada cuatro (4) meses, a través del informe de seguimiento y matriz de riesgos, en los diez (10) primeros días hábiles al corte del reporte. Reporta el resultado del seguimiento a la OCI, a través del informe de seguimiento y la Matriz de Riesgos Institucional en los quince (15) primeros días hábiles al corte. Publica el informe de seguimiento y la Matriz de Riesgos Institucional en la carpeta Unidad MIPG y la web de la entidad, en los quince (15) primeros días hábiles al corte.
TERCERA (OCI)	La evaluación a la Matriz de Riesgos Gestión se realiza según lo definido en el Plan Anual de Auditoría aprobado por el CICCI en cada vigencia, ya que dependerá del universo de auditoría y de priorización de procesos según la evaluación de los riesgos.	La evaluación a la Matriz de Riesgos de Seguridad Digital según lo definido en el Plan Anual de Auditoría aprobado por el CICCI en cada vigencia, ya que dependerá del universo de auditoría y de priorización de procesos según la evaluación de los riesgos.	La evaluación a la Matriz de Riesgos de Seguridad Digital según lo definido en el Plan Anual de Auditoría aprobado por el CICCI en cada vigencia, ya que dependerá del universo de auditoría y de priorización de procesos según la evaluación de los riesgos.

Fuente: Elaboración propia

** Nota: No se realiza la publicación del informe de seguimiento y la Matriz de Riesgos Institucional en la página web de la Entidad, dado que hacer públicos ciertos riesgos puede permitir que actores maliciosos exploten las vulnerabilidades antes de que se implementen soluciones, así mismo puede afectar la imagen reputacional de la Entidad.*

La presente Política, así como el SIGRIP está sujeto a las mejoras que la Alta Dirección o línea estratégica, consideré el proceso de mejora es continuo, y se nutre de los reportes que se generan en el monitoreo, seguimiento, evaluaciones y auditorías. Es sujeto de trasladarse a los planes de mejoramiento que se requieran, para atender a los hallazgos y no conformidades identificadas por la auditoría. También, deben tenerse en cuenta, desde el enfoque preventivo, las evaluaciones y los resultados del monitoreo.

11. ACCIONES POR SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

A continuación, se listan las actividades que la Entidad debe iniciar en caso de materialización de un riesgo, con el objetivo de incorporar las medidas necesarias según el tipo de riesgo identificado y garantizar una respuesta oportuna y efectiva.

La primera línea, además, deberá notificar a la segunda y tercera línea mediante correo electrónico o memorando, generando alerta sobre las posibles consecuencias. Esta comunicación debe incluir una descripción detallada de lo ocurrido, el impacto generado en los objetivos del proceso y en la Entidad, así como cualquier información relevante para la toma de decisiones.

Tabla 17. Acciones en caso de materialización.

TIPO DE RIESGO	ACCIONES
RIESGOS DE GESTIÓN, SEGURIDAD DE LA INFORMACIÓN Y FISCAL	La línea de defensa que detecte la materialización de un riesgo deberá informar de manera inmediata, mediante un medio oficial (memorando y/o informe), a las demás líneas de defensa y a la Oficina de Control Disciplinario Interno la situación presentada, con el fin de garantizar una comunicación oportuna y coordinada. Independientemente del origen de la identificación, la primera y segunda línea de defensa deberán iniciar las actividades correspondientes para la gestión del riesgo materializado
	La primera y Segunda línea deben identificar la causa raíz del riesgo materializado. Evaluar el impacto en los objetivos del proceso y en la Entidad (Económica, Reputacional)
	La primera línea de defensa, con el apoyo de la segunda línea, deberá formular y establecer un plan de acción basado en el diagnóstico de la situación presentada, documentándolo en el mapa de riesgos. Este plan debe incluir la identificación y ejecución de acciones correctivas orientadas a mitigar el impacto y prevenir recurrencias. Asimismo, cuando aplique, implementar las medidas para contener el riesgo materializado.
	La segunda línea de defensa (OAP) debe llevar a cabo un monitoreo mensual de las actividades propuestas, a su vez incluirá el evento presentado en el histórico de eventos materializados que se refleja en el informe de monitoreo que es remitido a la Oficina de control Interno.
	La tercera línea de defensa (OCI) deberá evaluar que los controles implementados para atender el riesgo formulado. Además, verificará las acciones adelantadas por la primera y segunda línea de defensa, asegurando que estas medidas mitiguen adecuadamente el impacto y prevengan la recurrencia del riesgo materializado.
INTEGRIDAD PÚBLICA	La primera línea debe informar a la Oficina de Control Disciplinario Interno, la segunda y tercera línea de defensa de la materialización del riesgo y generar alerta de las posibles consecuencias mediante correo electrónico o memorando. Efectuando una descripción detallada de lo ocurrido, contemplando el impacto generado a los objetivos del proceso y la Entidad por la materialización del riesgo.
	La primera línea con el apoyo de la segunda línea debe, basado en el diagnóstico de la situación presentada, establecer un plan de acción documentado en el mapa de riesgos. Así como identificar y ejecutar las acciones correctivas.
	La segunda línea de defensa (OAP) debe llevar a cabo un monitoreo mensual de las actividades propuestas, a su vez incluirá el evento presentado en el histórico de eventos materializados que se refleja en el Informe periódico.
	Tanto la segunda como la tercera línea de defensa debe verificar si se diseñó y ejecuto el plan de acción y se actualizó el mapa de riesgos.
	La línea de defensa que identifique la materialización debe informar a las autoridades internas y externas de la ocurrencia del hecho. Se debe contar con la asesoría y apoyo de la Dirección Jurídica y Contractual para el desarrollo de la notificación.

TIPO DE RIESGO	ACCIONES
	La tercera línea de defensa (OCI) debe evaluar que los controles sean efectivos y oportunos, y atiendan el riesgo formulado.

Fuente: Elaboración propia

El resultado del ejercicio debe socializarse a la Línea Estratégica mediante el CICCI, en un tiempo no mayor a 2 meses de identificada la materialización del riesgo, escenario en el que se debe establecer si es necesario algún tipo de reporte ante los organismos de control. La presentación ante el comité de la materialización del riesgo corresponde a la segunda línea en el evento que la materialización sea notificada por la primera línea de defensa y para los eventos detectados por la Oficina de Control Interno en los ejercicios de auditoría, la presentación estará a cargo de la tercera línea.

Un riesgo (gestión, fiscal, seguridad de la información) se ha materializado cuando la situación que se había identificado como posible (riesgo) ocurre realmente y genera un impacto negativo sobre los objetivos.

Para los Riesgos de Integridad Pública el riesgo se materializa siempre que se advierta un impacto sobre la reputación, la operación o de cumplimiento o que comprometa la ejecución del recurso. La consecuencia reputacional, surge cuando la organización se ve involucrada en denuncias o reportajes que la vinculan con prácticas poco íntegras, incumplimientos normativos o corrupción en general. La consecuencia legal inicia desde el mismo momento en que una parte vinculada es involucrada en procesos que puedan derivar en una sanción y el contagio se da cuando la involucrada es la parte relacionada. Finalmente, la consecuencia económica puede configurarse, incluso, desde el mismo momento en que hay retrasos en la ejecución del recurso, por conductas poco íntegras del ejecutor. Para los riesgos de LA/FT/FP aun cuando no haya consecuencias, toda operación sospechosa, incluso la intentada, debe ser objeto de reporte, al margen de la materialización del delito de lavado de activos.

La materialización del riesgo no debe confundirse con la ocurrencia del delito, falta o conducta generadora de responsabilidad fiscal. Es posible que el riesgo se haya materializado, es decir, que haya un impacto con consecuencias negativas para la entidad, incluso antes de la vinculación formal a procesos sancionatorios. También, es posible que el riesgo se materialice aun cuando la persona termine absuelta. Por lo anterior, los riesgos para la integridad no deben entenderse como tipos penales o disciplinarios, ni la materialización del riesgo implica un prejuzgamiento.

Toda la gestión del riesgo tiene como principales objetivos la identificación, medición, control y el monitoreo, con el propósito de prevenir, detectar y corregir. En ningún caso podrá derivar en juicios de responsabilidad o en la aplicación de sanciones. Ante un escenario de materialización de un riesgo, la respuesta institucional debe estar encaminada a asegurar la “continuidad del negocio[3]”, es decir, a asegurar que, a pesar del impacto que hubo en los objetivos derivados del riesgo que se materializa, estos se puedan cumplir.

12. INDICADORES CLAVE DE RIESGO

Los Indicadores Clave de Riesgos (KRI), hacen referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o

[3] Continuidad del negocio: El conjunto de actividades y procedimientos que mantienen en niveles aceptables el funcionamiento de la misionalidad de la Entidad y la prestación de sus servicios durante eventos que impidan de manera significativa sus procesos normales

menor exposición a determinados riesgos, esto asociado al cumplimiento de los objetivos de los procesos y por ende de los objetivos estratégicos. Un resultado desfavorable no necesariamente indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe analizar con el fin de identificar, estimar y monitorear la ocurrencia y severidad de los eventos y los factores, así como posibles amenazas, por lo que se constituyen en una herramienta de apoyo para el seguimiento y monitoreo de los riesgos, ya que pueden entregar señales de alerta temprana, así como detectar tendencias o cambios en los niveles de riesgo, lo que facilita que se incorporen acciones correctivas y preventivas para minimizar sus impactos frente a posibles materializaciones.

Los indicadores clave de riesgo para el JBJCM corresponden a los indicadores de Gestión que atienden a lo proyectado en el DYP.PR.04 Gestión de Indicadores, los cuales cuentan con su metodología de aplicación y permiten dar cumplimiento de las actividades críticas y por ende de los objetivos de los procesos como resultado de lo identificado en el DYP.PR.07.F.06 Contexto Estrategico por Procesos.

Se promoverá la identificación de un Indicador clave de riesgo por cada actividad critica detectada.

13. GESTIÓN DE OPORTUNIDADES

De acuerdo con los lineamientos establecidos en la ISO 9001:2015, las entidades deben establecer acciones para abordar los riesgos y oportunidades, para el primero de los casos, es decir los **riesgos** es necesario tener en cuenta que se presenta para aquellos casos que pueden generar una afectación de carácter potencialmente negativo, aspectos que han sido abordados en los numerales anteriores, para el segundo de los casos es decir las **oportunidades**, se entenderá para potenciales afectaciones que pudieren generar un impacto positivo.

De acuerdo con lo enunciado, la Entidad ha implementado la siguiente metodología para el tratamiento de oportunidades que se atenderá de manera secuencial, para lo cual el documento referente será la DYP.PR.07. F.0 **Matriz de Oportunidades Institucionales**:

13.1. Identificación de Oportunidades

El insumo principal para la identificación de oportunidades será la matriz **DOFA** del proceso, de donde se identifican las Oportunidades establecidas allí y que son entendidas como situaciones externas favorables a la organización, en este sentido previamente, se debe valorar si las oportunidades presentan afinidad, así las cosas, si se cuenta con 5 oportunidades, éstas podrían resumirse en una sola o en dos, esta situación solo se podrá dar si hace un análisis de afinidad entre las mismas, en caso de no poderse agrupar por afinidad, se debe hacer una valoración de cuales de las oportunidades son relevantes y solo en este momento ya fuese por afinidad o selección de las oportunidades relevantes, se da inicio a la construcción de la matriz.

Como mínimo cada proceso debe presentar una oportunidad, no obstante, si evaluada la DOFA del proceso, se identifican otras oportunidades que no se han contemplado, estas podrán solicitarse al proceso para su incorporación.

En caso de que se establezca más de una oportunidad, estas deben analizarse en filas independientes, tal y como se muestra a continuación:

Tabla 18. Matriz de Oportunidades Institucionales.

No OP	Proceso	Oportunidad
1	Nombre proceso	Oportunidad 1
2	Nombre proceso	Oportunidad 2

Fuente: Elaboración propia

Nota1: Estas son las tres primeras columnas de la Matriz de Oportunidades Institucionales.
Nota 2: Las oportunidades se deben redactar de manera positiva y deben iniciar con un verbo en infinitivo. (-ar, -er, -ir).

13.2. Calificación De Oportunidades

Al igual que los riesgos, las oportunidades se califican a través de probabilidad e impacto, para ello se entenderá por cada uno lo siguiente:

Probabilidad: Posibilidad de ocurrencia de la oportunidad, para ello se tendrán las siguientes escalas:

Tabla 19. Matriz de Oportunidades Institucionales.

Probabilidad	Probabilidad de Calificación
No se ha presentado en los últimos 5 años	1
Se presentó al menos una vez en los último 5 años	2
Se presentó al menos una vez en los últimos 2 años	3
Se presentó al menos una vez en el último año	4
Se ha presentado más de una vez en el año	5

Fuente: Elaboración propia

Impacto: Beneficios resultantes de la posible materialización de la oportunidad.

Tabla 20. Matriz de Oportunidades Institucionales.

Impacto	Impacto Calificación
Sin aportes al cumplimiento de las metas y objetivos institucionales, el mejoramiento y satisfacción de los usuarios.	1
Aporte mínimo al mejoramiento en la calidad de los servicios y satisfacción de los usuarios.	2
Aportes parciales al cumplimiento de las metas y objetivos institucionales.	3
Mejoramiento en la calidad del servicio y satisfacción de los grupos de valor.	4
Cumplimiento de las metas y objetivos institucionales favoreciendo la realización de las metas de gobierno y/o Imagen institucional favorecida en el orden nacional o regional por cumplimientos en la prestación del servicio a los usuarios o ciudadanos.	5

Fuente: Elaboración propia

En este sentido, se deben diligenciar los siguientes campos:

Tabla 21. Matriz de Oportunidades Institucionales.

No Op	Proceso	Oportunidad	Probabilidad (de lograr la oportunidad)		Evidencia de la probabilidad	Impacto (Beneficios obtenidos con la oportunidad)		Factor de la oportunidad (Probabilidad x Beneficio)
			Probabilidad	Calificación probabilidad		Impacto	Calificación del impacto	

Fuente: Elaboración propia

Nota1: La probabilidad y el impacto se seleccionan de una lista desplegable, la calificación de la probabilidad se genera de manera automática.
Nota 2: Cuando se califique la probabilidad, en el campo de evidencia de la probabilidad, se debe colocar la evidencia objetiva que soporta la frecuencia de la probabilidad seleccionada.
Nota 3: El factor de oportunidad, es un valor automático, que sale de multiplicar la calificación de la probabilidad y la calificación del impacto.

13.3. Escenario de Intervención

El escenario de intervención será resultante de la relación entre la Probabilidad vs Impacto, con lo cual aparecerá el escenario de intervención de la oportunidad, para ello se tendrá en cuenta lo siguiente:

- Si el factor de oportunidad presenta un valor mayor a 15, el plan de acción de la actividad debe desarrollarse en un plazo menor a seis meses.
- Si el factor de oportunidad presenta un valor entre 10 y 15, el plan de acción de la actividad debe desarrollarse entre seis meses y un año.
- Si el factor de oportunidad presenta un valor entre 5 y 9, el plan de acción de la actividad debe desarrollarse entre un año y dos años.
- Si el factor de oportunidad presenta un valor menor a 5, el plan de acción de la actividad debe desarrollarse en un plazo mayor a dos años o se debe tomar la decisión de no efectuar nada.

Tabla 22. Matriz de Oportunidades Institucionales.

Factor de la oportunidad (Probabilidad x Beneficio)	Escenario de intervención de la oportunidad	Actividad que se realizará	¿La actividad es técnica, financiera y jurídicamente viable? (Si la respuesta es SI a las tres opciones continúe a las siguientes columnas, si la respuesta es NO a una o a las tres opciones, replantee la actividad que se plantea realizar)
15	ACCIONES Y ACTIVIDADES A MEDIANO PLAZO (MAYOR A SEIS MESES)		SI

Fuente: Elaboración propia

Nota 1: La actividad a realizar debe corresponder a una acción objetiva, es decir que pueda ser evidenciable en su cumplimiento.
Nota 2: Es fundamental que la actividad que se pretenda realizar, presente tanto viabilidad técnica, financiera y jurídica, en este sentido en la columna que evalúa las viabilidades, en caso de que la respuesta fuese NEGATIVA, no se dará continuidad con la formulación de la oportunidad y quedará dicho registro en el matriz control, sujeta a futuras evaluaciones.

13.4. Desarrollo de la actividad

Las últimas cuatro columnas de la matriz corresponden al período en el cual se desarrollará la actividad, así como la evidencia del seguimiento y la determinación del beneficio real.

Tabla 23. Matriz de Oportunidades Institucionales.

Fecha inicio (DD/MM/AA)	Fecha fin (DD/MM/AA)	Evidencia del seguimiento	Seguimiento proceso	Seguimiento OAP	Seguimiento OCI
1/03/2022	30/10/2022				

Fuente: Elaboración propia

Nota 1: Las fechas en las cuales se desarrollarán las actividades, se relacionarán en el formato DD/MM/AA, es necesario que este período corresponda al escenario de intervención de la oportunidad, es decir, se debe tener en cuenta si la intervención es inmediata, o del corto, mediano y largo plazo, en caso de que el escenario de intervención es mayor a dos años, se debe colocar N.A., tanto en la fecha de inicio, como la de fin.
Nota 2: La evidencia del seguimiento, es un documento que debe dar fe de la realización de la actividad.
Nota 3: Cuando de manera inmediata se pueda establecer evidencia del éxito esta debe colocarse en el campo de verificación, esta situación se comprobará a través de la auditoría interna, en caso de que no se presente una mejora inmediata se colocará N.A., sin embargo, en futuras auditorías se comprobará el éxito de esta.

Una vez ha sido estructurada por los líderes de los procesos, esta debe remitirse a la Oficina de Planeación, quien será la encargada de la consolidación.

Desde la segunda línea de defensa se debe proceder con el seguimiento en la Matriz de Oportunidades Institucionales, así como la elaboración del informe periódico correspondiente. Se contará con el registro histórico de las oportunidades inactivas y cumplidas.

13.5. Reporte y Monitoreo

Tabla 24. Acciones y responsabilidades Gestión de Oportunidades.

GESTIÓN DE OPORTUNIDADES	
DESCRIPCIÓN ACCIÓN Y ENCARGADO	**TIEMPOS DE ENTREGA, REVISIÓN Y SEGUIMIENTO**
Los líderes de cada proceso o el enlace MIPG efectúa el reporte de la gestión de Oportunidades junto con los seguimientos actualizados.	Cada seis (6) meses, con corte a 30 junio, 31 de diciembre de cada año, y cargando los soportes en el repositorio destinado por la Oficina Asesora de Planeación a través del correo electrónico institucional, dentro de los diez (10) primeros días hábiles del mes siguiente a las fechas de corte ya mencionadas.
La Oficina Asesora de Planeación efectúa el alertamiento del respectivo reporte.	Realiza el alertamiento del corte del periodo para la entrega de información, dentro de los seis (6) días hábiles previos al corte a través de correo electrónico
La Oficina Asesora de Planeación efectúa el alertamiento de incumplimiento.	Realiza alertamiento del incumplimiento a los procesos que no reportaron oportunamente, en los doce (12) primeros días hábiles al corte, a través de correo electrónico.
La Oficina Asesora de Planeación realiza el seguimiento y retroalimentación al avance de la implementación de los controles y de las acciones formuladas en la Matriz de Oportunidades institucionales.	Cada seis (6) meses, a través del informe de seguimiento y matriz de riesgos, en los quince (15) primeros días hábiles del mes siguiente a las fechas de corte del reporte.
La Oficina Asesora de Planeación realiza el reporte del resultado de seguimiento a la Oficina de Control de Interno.	En los quince (15) primeros días hábiles al corte, a través del informe y la matriz de riesgos institucional.
La Oficina Asesora de Planeación publica el informe	

GESTIÓN DE OPORTUNIDADES	
DESCRIPCIÓN ACCIÓN Y ENCARGADO	**TIEMPOS DE ENTREGA, REVISIÓN Y SEGUIMIENTO**
de seguimiento y la Matriz de Oportunidades Institucional en la “Unidad MIPG”.	El último día hábil del mes siguiente al corte.
La OCI realiza evaluación a la Matriz de Oportunidades Institucionales.	Según lo definido en el Plan Anual de Auditoría.

Fuente: Elaboración propia OAP

14. BIBLIOGRAFÍA

- International Standard Organization. (2018). Gestión del riesgo. Principios y Directrices ISO 31000:2018.
- International Standard Organization. (2015). Sistemas de Gestión de la Calidad ISO 9001:2015.
- Función Pública. (2018). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas de Función Pública (V4).
- Función Pública. (2020). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (V5).
- Veeduría Distrital. (2019). Metodología Prevención de Riesgos de Soborno en Entidades Públicas
- Ministerio de Tecnologías de la Información y las Comunicaciones – TICs. (2021). Modelo de Seguridad y Privacidad de la Información – MinTIC, Anexo 4. "Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas".
- Ley 1474 artículo 73 de 2011. Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano Primer componente.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 648 de 2017. Por el cual se modifica y adiciona el Decreto 1083 de 2015, reglamentaria Único del Sector de la Función Pública.
- Decreto 1499 de 2017. Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades
- International Standard Organization. (2022). Seguridad de la Información, Ciberseguridad y Protección de la Privacidad - Controles de Seguridad de la Información. ISO 27002:2022

15. ANEXO 1. CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Introducción

Como resultado de la metodología de investigación que ha venido implementando el *Semillero de Investigación de la Academia de la Gestión Pública* desde el año 2018, fue posible identificar los principales *puntos de riesgo fiscal* y *circunstancias inmediatas* de dichos riesgos, mediante el estudio de: i) los avances que los diferentes órganos de control tienen frente a la definición de riesgo fiscal y la identificación de los principales riesgos fiscales en sus sujetos vigilados, ii) el estudio de fallos con responsabilidad fiscal en firme, emitidos tanto por contralorías territoriales como por la Contraloría General de la República.

Así las cosas, los *puntos de riesgo fiscal* que se enuncian en este catálogo indicativo y enunciativo corresponden a actividades que representan gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública y que potencialmente pueden generar un efecto dañoso al patrimonio público.

Este listado enunciativo y no restrictivo, también posibilita identificar y conocer las *Circunstancias Inmediatas* más comunes en la gestión pública, que se derivan de los *Puntos de Riesgo Fiscal.*

Así las cosas, como resultado del análisis de más de 130 fallos con responsabilidad fiscal tanto de contralorías territoriales como de la Contraloría General de la República, fue posible identificar 50 *puntos de riesgo fiscal* e igual número de *circunstancias inmediatas,* así*:*

Tabla 25. Puntos de riesgo fiscal.

Id Referencia	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Circunstancia Inmediata** *Situación **por la que** se presenta el riesgo*
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron

Id Referencia	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Circunstancia Inmediata** *Situación **por la que** se presenta el riesgo*
19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista

Id Referencia	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Circunstancia Inmediata** *Situación **por la que** se presenta el riesgo*
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2022[4]

[4] Este catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias Inmediatas, es el resultado del análisis de investigaciones previas y del estudio detallado de información sobre:
(i) Fallos con responsabilidad fiscal, en firme, emitidos en los últimos 3 años, por una muestra de 10 de las contralorías territoriales mejor calificadas en 2020, según el criterio de desempeño integral, el cual corresponde a evaluación realizada por la Auditoría General de la República.
(ii) Muestra aleatoria de fallos con responsabilidad fiscal, en firme, emitidos por la Contraloría General de la República en los últimos 3 años.
(iii) Listado de hallazgos fiscales por temáticas, consolidado por la Auditoría General de la República, 2021.

16. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
07/07/2019	1	Se adopta la Política de Administración de Riesgos a través de la Resolución 240 de 2019.
09/09/2020	2	Se actualiza la Política de Administración de Riesgos de acuerdo con los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V4.2018.
27/12/2021	3	Actualización del documento a integridad con base a los lineamientos suministrados 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 5 emitida en diciembre de 2020".
31/08/2022	4	Actualización del numeral 5.2 Riesgos de Seguridad de la Información, en cuanto a la gestión de esta tipología de Riesgos. Inclusión de la Gestión de Oportunidades en el numeral 10. Actualización del numeral 8 Reporte de los Mapas de Riesgos en cuanto a los términos de ejecución de actividades. Actualización del numeral 5.1.1 Identificación del Riesgo con relación al análisis de factores inclusión de la Clasificación de Riesgos por factor e identificación de causas numeral 5.1.2.
29/12/2023	5	Ajuste de términos asociados a la Gestión de Oportunidades. Inclusión de Capitulo de Riesgos Fiscales, se complementan las definiciones y metodología de la gestión de cada tipología de riesgo con el fin de aclarar su ejecución. Se da cobertura a SARLAFT en los Riesgos de Corrupción.
8/10/2024	6	Cambios en capítulo de Riesgos de Seguridad de la Información respecto a la redacción de controles. Ajustes en la introducción respecto a Riesgos de Seguridad de la Información. Ajuste a Roles y responsabilidades por la adopción del Portal MIPG.
07/01/2026	7	Actualizado con base a la emisión de la "Guía para la Gestión Integral del Riesgo en Entidades Públicas" versión 7 de la Función Pública, en los siguientes aspectos: 1. Se unifica la estructura conceptual y metodológica para la gestión del riesgo bajo un enfoque integral, con elementos comunes aplicables a todas las tipologías de riesgo. 2. Se amplían los términos y definiciones en concordancia con la aplicación de los nuevos elementos. 3. Se profundiza el análisis sobre apetito del riesgo en el marco COSO-ERM (2017) que precisa y profundiza los conceptos de riesgo, gestión del riesgo y niveles de madurez del riesgo. 4. Se agregan contenidos conceptuales y ejemplos relacionados con la gestión preventiva de riesgos. 5. Se modifica y actualiza el capítulo de riesgos asociados a posibles actos de corrupción, incorporando el Sistema de Gestión de

FECHA	VERSIÓN	DESCRIPCIÓN
		Riesgos para la Integridad Pública - SIGRIP, de acuerdo con el componente programático de la Estrategia Institucional para la Lucha Contra la Corrupción, temática 1 Administración del Riesgo indicado en el Anexo Técnico de los Programas de Transparencia y Ética Pública. 6. Se actualizan contenidos relacionados con los riesgos de seguridad de la información, desplegando la totalidad de los pasos metodológicos.

17. AUTORIZACIONES

PROCESO			
ELABORÓ		**APROBÓ**	
Nombre(s)	Pablo Leonardo Molano Parra	**Nombre(s)**	Sandra Marcela Torres Forero
Cargo(s): Contratista MIPG-Oficina Asesora de Planeación		**Cargo(s):** Jefe Oficina Asesora de Planeación	

OFICINA ASESORA DE PLANEACIÓN					
REVISÓ		**APROBÓ**		**PUBLICÓ**	
Nombre(s)	José David Hernández Jina Paola González	**Nombre(s)**	Sandra Marcela Torres Forero	**Nombre(s)**	José David Hernández
Cargo(s): Contratistas MIPG- Oficina Asesora de Planeación		**Cargo(s):** Jefe Oficina Asesora de Planeación		**Cargo(s):** Contratista MIPG-Oficina Asesora de Planeación	