2025

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

ALCALDÍA DE
BUCARAMANGA

MUNICIPIO DE BUCARAMANGA

Versión 8.0

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA** (aprobación)	**DESCRIPCIÓN DE AJUSTES**	**RESPONSABLE** (Cargo según Manual de Funciones)
0.0	29-03-2017	Original	Profesional Especializado
1.0	30-05-2017	Se incluyeron los riesgos transversales y códigos de formatos y guía.	Profesional Especializado
2.0	18-01-2019	Actualización documental, teniendo en cuenta la Guía para la administración del riesgo del DAFP 2018	Profesional Especializado
3.0	28-04-2021	Actualización documental, teniendo en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP 2020.	Profesional Especializado
4.0	27-07-2021	Actualización en los numerales 8. Responsabilidad y Roles – Segunda Línea de Defensa y 9.4 Lineamientos Riesgos de Seguridad de la Información.	Profesional Especializado
5.0	9-11-2021	Actualización numeral 9.3 lineamientos riesgos relacionados con posibles actos de corrupción, de acuerdo con la Guía para la administración del riesgo del DAFP versión 4 de 2018.	Profesional Especializado
6.0	24-11-2022	Se incluyó en el numeral 9.4 Lineamientos Riesgos de Seguridad de la Información la Matriz Mapa Riesgos de Seguridad de la Información F-TIC-1400-238,37-047	Profesional Especializado
7.0	08-09-2023	Actualización documental, teniendo en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP 2022. Se incluyó el capítulo 10. Lineamientos para el análisis de riesgo fiscal.	Profesional Especializado
8.0	10-07-2025	Introducción, Objetivo, Objetivos específicos, Alcance, se incluyeron definiciones, Contexto de la entidad, Normatividad, Lineamientos de la política de administración de riesgos -Niveles de Responsabilidad y Metodología General para la Gestión del Riesgo (Reorganizó). Aprobado en Comité Institucional de Coordinación de Control según acta No.8 del 25 de junio de 2025 y en Comité Institucional de Gestión y Desempeño según acta No. 3 del 25 de junio de 2025	Profesional Especializado

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

MUNICIPIO DE BUCARAMANGA

Secretaría de Planeación	Planeación y Direccionamiento Estratégico
	Mejoramiento Continuo

TABLA DE CONTENIDO

ALCALDÍA DE
BUCARAMANGA

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

La Alcaldía de Bucaramanga, en su compromiso con la gestión pública eficiente, ética y transparente, reconoce la importancia de contar con un enfoque preventivo que permita anticiparse a situaciones que puedan afectar el cumplimiento de sus funciones y el logro de sus objetivos estratégicos. En este sentido, la gestión del riesgo se consolida como una herramienta fundamental para fortalecer la toma de decisiones, proteger los recursos públicos y mejorar la calidad de los servicios ofrecidos a los ciudadanos.

Con fundamento en la normatividad vigente y en la metodología establecida por el Departamento Administrativo de la Función Pública mediante la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6 – noviembre de 2022*, la Administración Municipal presenta la Política de Administración de Riesgos versión 8.0. Este instrumento estratégico establece los lineamientos institucionales necesarios para identificar, analizar, tratar, monitorear y evaluar los riesgos que puedan interferir en el desempeño institucional, contribuyendo a reducir su vulnerabilidad.

La Política de Administración de Riesgos representa el compromiso del equipo directivo con la generación de una cultura organizacional basada en la prevención, la responsabilidad y el buen gobierno. Su implementación abarca todos los niveles de la Entidad y se articula con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno – MECI, y el enfoque por líneas de defensa.

Este documento promueve la participación activa de los servidores públicos y contratistas, quienes, desde sus funciones y responsabilidades, aportan a la construcción de un entorno institucional resiliente, con capacidad de respuesta ante eventos adversos. Así, la Alcaldía de Bucaramanga avanza hacia el fortalecimiento del sistema de control interno, la mejora continua de sus procesos y la consolidación de una administración orientada a resultados y al servicio efectivo de la ciudadanía.

OBJETIVO

Definir los lineamientos de la política integral de gestión del riesgo en la Alcaldía de Bucaramanga que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir en el cumplimiento de sus funciones y objetivos estratégicos institucionales, con el propósito de gestionar los riesgos identificados que permita a la entidad contar con un enfoque preventivo para la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a los ciudadanos del municipio de Bucaramanga.

1.2 OBJETIVOS ESPECÍFICOS

a) Orientar y fortalecer la toma de decisiones oportuna a través de un marco metodológico para la **identificación, análisis y evaluación de riesgos** al interior de la Administración Municipal, que puedan afectar el cumplimiento de los objetivos institucionales y la prestación efectiva de los servicios a los ciudadanos.
b) **Fortalecer la capacidad institucional para la protección de los recursos públicos,** asegurando su uso eficiente, transparente y orientado al beneficio de la ciudadanía.
c) **Garantizar la integración de la gestión del riesgo en los procesos estratégicos, misionales, de apoyo y de control** de la entidad, asegurando una visión transversal y preventiva.
d) **Promover una cultura organizacional orientada a la gestión proactiva del riesgo**, encaminada a prevenir y administrar los riesgos, que faciliten el desarrollo institucional, manteniendo la buena imagen y las buenas prácticas en todos los niveles de la entidad.

e) **Establecer mecanismos de seguimiento, monitoreo y mejora continua del sistema de gestión del riesgo,** que permitan evaluar la efectividad de las acciones implementadas y realizar los ajustes necesarios.
f) Determinar roles y responsabilidades de los servidores de la entidad (esquema de las líneas de defensa) en la gestión del riesgo de gestión en la Alcaldía de Bucaramanga.

ALCANCE

La Política de Administración de Riesgos aplica al direccionamiento estratégico, al modelo de operación por procesos, así como a los programas y proyectos que desarrolla la entidad para su cumplimiento misional.

TERMINOS Y DEFINICIONES

A continuación, se relaciona términos y definiciones, necesarios para la comprensión de los lineamientos de la política integral de gestión del riesgo:

- **Activo**: en el contexto de seguridad de la información 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.
- **Amenazas**: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **Apetito del 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. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública, se clasifican en bienes de uso público y bienes fiscales, definidos así:
  a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional (las calles, plazas, puentes, vías, parques etc).
  b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc).
- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Tratándose de riesgo fiscal, se usa el término circunstancia inmediata.

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

- **Causa Raíz riesgo fiscal (Causa Eficiente o Causa Adecuada):** Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

- **CICCI:** Comité Institucional de Coordinación de Control Interno.

- **Circunstancia Inmediata:** Situación o actividad por la que se presenta el riesgo, pero no constituye la causa principal o básica (causa raíz) del riesgo fiscal.

- **Confidencialidad**: propiedad de la información que la hace no disponible, o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento, o un beneficio.
- **Control:** Medida que permite reducir o mitigar un riesgo.

- **Disponibilidad**: Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Efecto:** Es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.
- **Evento Potencial:** Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. Para el riesgo fiscal, el evento potencial es equivalente a la causa raíz.
- **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.
- **Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales.
- **Impacto:** Son las consecuencias que puede ocasionar a la organización la materialización del riesgo, que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

  Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.
- **Integridad**: propiedad de exactitud y completitud.
- **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. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.
- **Mapa de riesgos:** documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).
- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, que transforma elementos de entrada en elementos de salida para generar un valor.
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Programa de Transparencia y Ética Pública – PTEP:** programa de cumplimiento, mediante el cual la entidad define acciones estratégicas para promover al interior de la organización, una cultura de la legalidad e identificar, medir, controlar y monitorear los riesgos para la integridad que se presentan en el desarrollo de su misionalidad.

- **Puntos de riesgo fiscal:** Son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.
- **Recurso público:** Entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **Riesgo de corrupción**: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo fiscal:** Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Riesgo para la integridad pública:** Posibilidad de afectación económica o reputacional para la entidad u organización por no ejercer con integridad el servicio público debido a comportamientos y prácticas que atenten contra la moralidad administrativa o aquellas relacionadas con la corrupción, entre las que se encuentran el fraude, el soborno y la no declaración de conflictos de interés.
- **Riesgo de LA/FT/FP:** Posibilidad de afectación económica o reputacional para la entidad u organización por ser utilizada, en forma directa o indirecta, como instrumento para lavado de activos (LA), financiación del terrorismo (FT) y la proliferación de armas de destrucción masiva (FP).
- **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.
- **Riesgo Inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite 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.
- **Severidad:** Es la magnitud de las posibles consecuencias adversas del riesgo.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

CONTEXTO ENTIDAD

Bucaramanga, capital del departamento de Santander, fue fundada el 22 de diciembre de 1622. Está ubicada geográficamente en una terraza inclinada de la Cordillera Oriental, en las coordenadas 7°08′ de latitud norte y 73°08′ de longitud oeste. Limita al norte con el municipio de Rionegro, al este con Matanza, Charta y Tona, al sur con Floridablanca, y al oeste con San Juan de Girón. Su localización en una región montañosa, rica en biodiversidad, le confiere condiciones naturales únicas que han sido integradas en la planificación urbana y ambiental, con el objetivo de promover el desarrollo sostenible y la preservación del patrimonio natural.

El **contexto territorial** del municipio contempla elementos fundamentales para una gestión integral. Bucaramanga está dividida política y administrativamente en 17 comunas, que agrupan 219 barrios, 3 corregimientos y 36 asentamientos urbanos. El área total del municipio es de 165 km², de los cuales 79,2 km² corresponden al casco urbano y 85,5 km² a la zona rural.

En cuanto a su **composición demográfica**, Bucaramanga presenta una densidad poblacional de 4.024,05 habitantes por kilómetro cuadrado. La población total proyectada para el año 2024 fue de 619.703 habitantes, lo que representa aproximadamente el 1,2 %

de la población nacional y el 26,07 % del total del departamento de Santander, según el Censo Nacional de Población y Vivienda (DANE, 2018).

Desde el punto de vista **económico**, la ciudad muestra una marcada orientación hacia el sector terciario. Las actividades de servicios representan el 81,2 % del valor agregado total del municipio ($13.334.098 millones). Le siguen las actividades del sector secundario (industria y construcción), que aportan un 18,49 % ($3.036.945 millones), y finalmente el sector primario (agropecuario y minería), con una participación del 0,31 % ($50.818 millones).

MISIÓN	VISIÓN
Somos una entidad territorial al servicio de los ciudadanos que garantiza el ejercicio de sus derechos y el cumplimiento de sus deberes, promueve el bienestar y desarrollo humano, con oportunidad, equidad, transparencia, responsabilidad social, económica y ambiental, soportada en una gestión institucional innovadora y colaborativa, con un talento humano comprometido con su labor como Servidor Público.	En 2034 Bucaramanga Ciudad Región será un territorio referente a nivel nacional en materia de cultura ciudadana, seguridad, competitividad y gestión sostenible de sus áreas estratégicas; dinamizando su desarrollo desde la ciencia, la tecnología y la innovación, mediante acuerdos intersectoriales eficientes para mejorar la calidad de vida de todas las personas que lo habitan.

Tabla 1. Objetivos Estratégicos de la Entidad

OBJETIVOS ESTRATEGICOS DE LA ENTIDAD
TERRITORIO SEGURO QUE INTEGRA
Se constituye en el soporte para reconocer en Bucaramanga el sentido de lo humano como valor estructural, promoviendo el reconocimiento de la diferencia, la equidad, la inclusión social, la adquisición y el fomento de las capacidades necesarias para acceder al bienestar y mejorar la calidad de vida de los habitantes en las zonas urbanas y rural.
TERRITORIO SEGURO QUE PROGRESA
Se constituye un territorio atractivo para desplegar y articular proyectos locales, regionales, nacionales e internacionales que potencien la competitividad urbana y rural; desde el desarrollo empresarial, el empleo, el turismo, la ciencia, la tecnología, la innovación y la inclusión social.
TERRITORIO SEGURO Y SOSTENIBLE
Se constituye en la promoción de un desarrollo urbano y rural que garantice la preservación y gestión sostenible de los recursos naturales, el reconocimiento y la mitigación del cambio climático, la protección del medio ambiente, de los derechos y bienestar animal y la promoción de estilos de vida saludables.
TERRITORIO SEGURO QUE GENERA VALOR
Se constituye en el escenario para la articulación y la construcción de un sistema gubernamental sólido y eficiente, basado en principios de transparencia, competencia y eficacia en la gestión pública, cuya finalidad sea impulsar la modernización y profesionalización del gobierno local, fomentando la rendición de cuentas, la responsabilidad y la calidad en la prestación de servicios públicos. Además, de promover una cultura de servicio orientada al ciudadano, donde la atención y satisfacción de las necesidades de la comunidad sean prioritarias mostrando así una mayor confianza y participación de todos.
TERRITORIO SEGURO QUE PROTEGE
Se constituye la seguridad en un pilar fundamental de la convivencia ciudadana a partir de un enfoque multidimensional, la renovación y articulación de las instituciones públicas, para construir entornos urbanos y rurales donde las personas se sientan protegidas y puedan ejercer y gozar libremente de sus derechos y el cumplimiento de sus deberes; desde la corresponsabilidad.

Tabla 2. Análisis interno y externo especifico de la entidad

Análisis interno y externo especifico de la entidad		
CONTEXTO EXTERNO	Económicos y financieros	Recursos de inversión, liquidez, mercados, desempleo, competencia, presupuesto de funcionamiento, infraestructura, capacidad instalada, CONPES, austeridad del gasto, sistemas de registro SUE
	Políticos	Cambios de gobierno, legislación, políticas públicas, regulación, objetivos de Desarrollo Sostenible

	Sociales y culturales	Demografía, responsabilidad social, orden público, seguridad de los servidores públicos, conflicto de intereses, prevención corrupción, pandemias, ODS
	Tecnológicos	Avances en tecnología, Gobierno Digital, Interoperabilidad de los sistemas de información de gobierno, plataformas tecnológicas, requisitos de MinTic, seguridad de la información, servidores internos de la Entidad (Intranet, SIGC, Página Web institucional), inteligencia artificial (AI), análisis masivo de datos (Big data), Tecnologías de 4 revolución industrial (CONPES 3975), Confidencialidad, integridad y disponibilidad de los activos de información, Carpeta ciudadana, ciudadanos digitales, teletrabajo
	Medio Ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible, proximidad a los cerros, desastres naturales, contaminación, epidemias, pandemias
	Comunicación externa	Mecanismos y herramientas virtuales utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad
	Evento externo	Situaciones externas que afectan la entidad (atentados, vandalismo y orden público)
	Financieros	Recursos, necesidades de las dependencias, plan anual de adquisiciones, apropiación de recursos, comunicación entre las dependencias intervinientes en el proceso presupuestal.
	Talento Humano	Disponibilidad del personal, seguridad y salud ocupacional, Planta de personal, competencias del personal a partir de la implementación del Modelo Integrado de Planeación y Gestión MIPG, desarrollo de habilidades, motivación e involucramiento del personal, concurso de méritos para proveer los cargos en provisionalidad, incorporación de jóvenes profesionales
CONTEXTO INTERNO	Procesos	Apropiación Modelo Integrado de Planeación y Gestión MIPG, SIGC
	Tecnología	Integridad y Seguridad de los datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, Herramientas y aplicativos internos, servidores internos de la Entidad (Intranet, SIGC, Página Web), nube privada, riesgos de seguridad de la información
	Estratégicos	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo
	Comunicación interna	Canales internos utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones
	Diseño del proceso	Planes, programas, proyectos y presupuestos articulados, claridad en la descripción del alcance y objetivo del proceso, Riesgos institucionales integrados a los procesos, Procedimientos y flujos descritos
	Interacciones con otros procesos	Responsabilidad, autoridad y funciones, trabajo en equipo entre los procesos, políticas de operación. Articulación de la gestión del conocimiento con los procesos
CONTEXTO INTERNO DEL PROCESO	Procedimientos asociados	Actualización, socialización, procedimientos entre procesos
	Responsables del proceso	Grado de autoridad, responsabilidad compartida de los funcionarios frente al proceso, coordinación de los procesos, control de la
	Comunicación entre los procesos	Mecanismos de articulación entre los procesos (reuniones, canales, mecanismos de seguimiento).
	Activos de Seguridad Digital del	Procedimientos y estructura de matrices inventario de activos de información, Riesgos de Seguridad de la información

NORMATIVIDAD

- Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado; en el literal f del Artículo 2 establece como uno de los objetivos del Sistema de Control interno: definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.
- Ley 489 de 1998 Estatuto básico de organización y funcionamiento de la Administración Pública.

- Decreto 4485 de 2009, por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos Generales literal g) “establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad” cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder”. Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

- Ley 2195 de 2022, por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.

- Decreto 1122 del 30 de agosto de 2024 y su Anexo Técnico, por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública.

- Norma Técnica Colombiana NTC ISO 9001. Especifica los requisitos para la implementación de un Sistema de Gestión de la Calidad dirigido a garantizar la satisfacción del cliente, en el numeral 6.1 define que las Organizaciones deben establecer las acciones para abordar los riesgos y oportunidades, proporcionales al impacto potencial en la conformidad con los productos y servicios.

- Decreto 1083 de 2015, por el cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Título 23 Art. 2.2.23.1 - Adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública NTCGP 1000 Versión 2009, la cual establece las generalidades y los requisitos mínimos para establecer, documentar, implementar y mantener un Sistema de Gestión de la Calidad en los organismos, entidades y agentes obligados conforme al artículo 2° de la Ley 872 de 2003. La Norma Técnica de Calidad en la Gestión Pública, NTCGP 1000 versión 2009 es de obligatoria aplicación y cumplimiento. Art. 2.2.23.2. El establecimiento y desarrollo del Sistema de Gestión de la Calidad en los organismos y entidades públicas a que hace referencia el artículo 2° de la Ley 872 de 2004, será responsabilidad de la máxima autoridad de la entidad u organismo correspondiente y de los jefes de cada dependencia de las entidades y organismos, así como de los demás empleados de la respectiva entidad.

- Resolución 193 del 5 de mayo de 2016 de la Contaduría General de la Nación, incorpora, en los Procedimientos Transversales del Régimen de Contabilidad Pública, el Procedimiento para la evaluación del control interno contable.

- Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.

- Decreto 1499 de 2017, por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Resolución No. 0139 del 17 de abril de 2023, por la cual se adopta y actualiza la Política Institucional de Seguridad y Privacidad de la Información para el municipio de Bucaramanga.

- Norma Internacional ISO 31000:2018 “Administración/Gestión de riesgos — Lineamientos guía”

- Guía para la Administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad digital. Versión 4 de 2018 de la Función Pública

- Política de Operación Riesgos de la Función Pública, 2018

- Anexo 4 de la Guía DAFP 2018 - Lineamientos para la gestión de riesgos de seguridad de la información en Entidades Públicas.

- Ley 610 de 2000, por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las Contralorías.

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 – noviembre 2022 de la Función Pública

LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

6.1 NIVELES DE RESPONSABILIDAD

Tabla 3. Responsabilidad y Roles

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Estratégica	Alta Dirección - Alcalde Municipal, Comité Institucional de Coordinación de Control Interno	• Establecer y aprobar la Política de Administración de Riesgos y su actualización. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la Entidad y que puedan generar cambios en la estructura de riesgos y controles. • Evaluar el estado del sistema de control interno y aprobar las modificaciones actualizaciones y acciones de fortalecimiento de este.
Primera Línea	Líderes de Proceso y equipo de trabajo	• Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera, con énfasis en la prevención del daño antijurídico. • Definir, aplicar y hacer monitoreo a los controles para mitigar los riesgos identificados, alineado con las metas y objetivos de la Entidad y proponer mejoras a la gestión del riesgo en su proceso. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Realizar las acciones necesarias con su respectivo monitoreo, con el fin de evitar la materialización de los riesgos que se encuentren en valoración baja y moderada. • Informar a la Secretaría de Planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo y solicitar los respectivos ajustes, inclusión y actualización de los mapas de riesgos de su proceso. • Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.
Segunda Línea	Secretaría de Planeación y Área de la TIC	**Secretaría de Planeación:** • Asesorar en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración de riesgos institucionales. • Consolidar los Mapas de Riesgos y presentarlos para análisis, aprobación y seguimiento ante el Comité Institucional de Coordinación de Control Interno y Comité de Gestión y Desempeño Institucional. • Solicitar la publicación de los Mapas de Riesgos en la página web institucional. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de procesos. **Área de la TIC:** • Asesorar a los líderes de proceso en la identificación de los riesgos de seguridad de la información e implementación de los controles definidos. • Consolidar los riesgos asociados a riesgos de seguridad de la información y presentarlos para análisis, aprobación y seguimiento ante

		el Comité Institucional de Coordinación de Control Interno y Comité de Gestión y Desempeño Institucional. • Publicar los Mapas de Riesgos en la página web institucional
Tercera Línea	Oficina de Control Interno de Gestión	• Presentar al Comité Institucional de Gestión y Desempeño, el monitoreo a la eficacia de los controles de los riesgos de seguridad de la información de los procesos. • Asesorar y orientar sobre la metodología para la identificación, análisis y valoración del riesgo. • Analizar el diseño e idoneidad de los controles establecidos en los procesos. • Realizar seguimiento a los riesgos consolidados en los mapas de riesgos (dos veces al año), de conformidad con el Plan Anual de Auditoría. • Recomendar mejoras a la política de administración del riesgo.

6.2 METODOLOGÍA GENERAL PARA LA GESTIÓN DEL RIESGO

La metodología para la administración del riesgo requiere, en primer lugar, un análisis del estado actual de la estructura y gestión del riesgo en la Entidad. Este análisis debe realizarse desde una perspectiva estratégica, considerando la aplicación de los cuatro (4) pasos fundamentales para su desarrollo. Posteriormente, es necesario definir e implementar estrategias de comunicación y socialización que se apliquen de manera transversal en toda la Entidad, de modo que su efectividad pueda ser evidenciada a través del monitoreo y seguimiento al cumplimiento de la política de administración de riesgos adoptada por la Alcaldía.

Figura 1. Metodología General para la Gestión del Riesgo

Fuente: Función Pública 2025

A continuación, se definen los pasos para la adecuada gestión del riesgo en la Alcaldía de Bucaramanga, que deberán seguir los líderes de los procesos y sus equipos de trabajo, al inicio de cada vigencia**:**

6.2.1 Identificación y Descripción del Riesgo

A continuación se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la operación de la entidad, desde diferentes ámbitos organizacionales, bajo la comprensión del modelo de procesos aplicable, que puede variar por la naturaleza, funciones, estructura organizacional, grupos de valor que atiende, recursos y otras particularidades que permiten cumplir con la misionalidad en cada una de las entidades, en los diferentes órdenes y niveles de la administración pública.

6.2.1.1 Identificación de los Puntos de Riesgo. Son actividades dentro de la cadena de valor (insumos, procesos, productos, resultados e impacto) donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Para llevar a cabo este análisis se debe considerar la estructura del proceso y la forma como participa dentro de la cadena de valor o ciclo de los procesos para la entrega de productos y servicios públicos.

Figura 2. Cadena de Valor

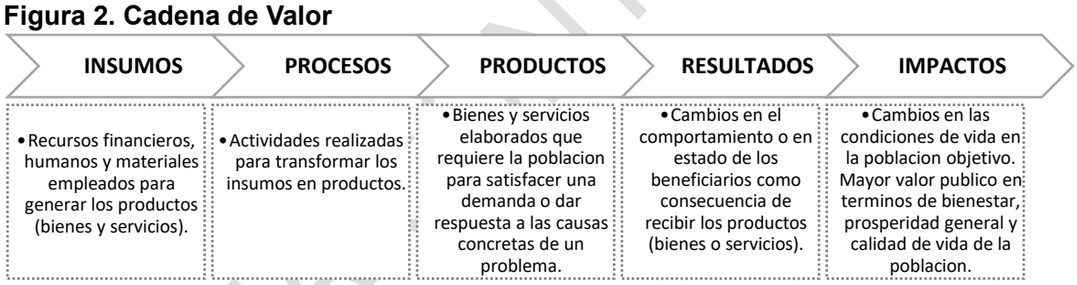


Tabla 4. Puntos de riesgos de los procesos

PUNTOS DE RIESGOS DE LOS PROCESOS
1. Operativos: Provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias.
2. Recurso Humano: Se asocian a la cualificación, competencia y disponibilidad de personal requerido para realizar un proyecto o función.
3. Financieros: Relacionados con el manejo de recursos que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes.
4. Cumplimiento y conformidad: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
5.Tecnológicos: Relacionados con la capacidad tecnológica para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
6. De Seguridad de la Información: Se asocia a la disponibilidad, confiabilidad e integridad de la información institucional.
7. De comunicación: Relacionados con los canales, medios y oportunidades para informar durante las diferentes etapas de un proyecto.

8. Contractual: Relacionados con los atrasos o incumplimientos de las etapas contractuales en cada vigencia.

6.2.1.2 Identificación de áreas de Impacto. El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional

- **Afectación Reputacional.** Es el deterioro de la relación con los grupos de valor como resultado de una percepción negativa sobre el comportamiento de la entidad.

✓ Perdidas por la disminución de la confianza en la integridad de la entidad que surge cuando su buen nombre es afectado.

✓ Opinión publica negativa sobre el servicio prestado.

✓ La afectación reputacional puede derivar en acciones que fomenten la creación de una mala imagen o un posicionamiento negativo en la mente de los ciudadanos.

Factores:

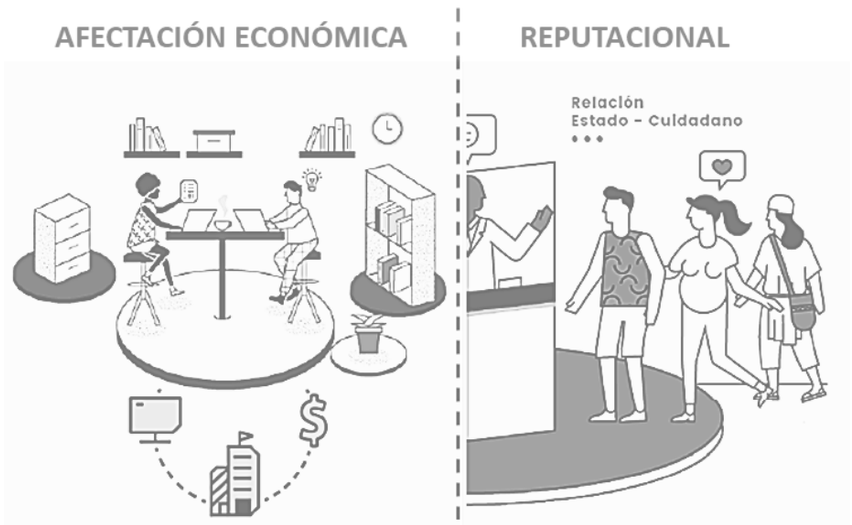
✓ Fallas en la comunicación
✓ Factores externos
✓ Fallas relevantes en los servicios y productos
✓ Insatisfacción de los grupos de valor

- **Afectación económica o presupuestal.** Se relaciona con los recursos económicos de la entidad, principalmente de la eficiencia y transparencia en el manejo de los recursos.

Factores:

✓ Recursos públicos mal utilizados

✓ Desvío de presupuesto
✓ Pérdidas por actos de corrupción



6.2.1.3 Identificación de áreas de Factores de Riesgo. Son las fuentes generadoras de riesgos. En la Tabla 5 encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

Tabla 5. Factores de riesgo

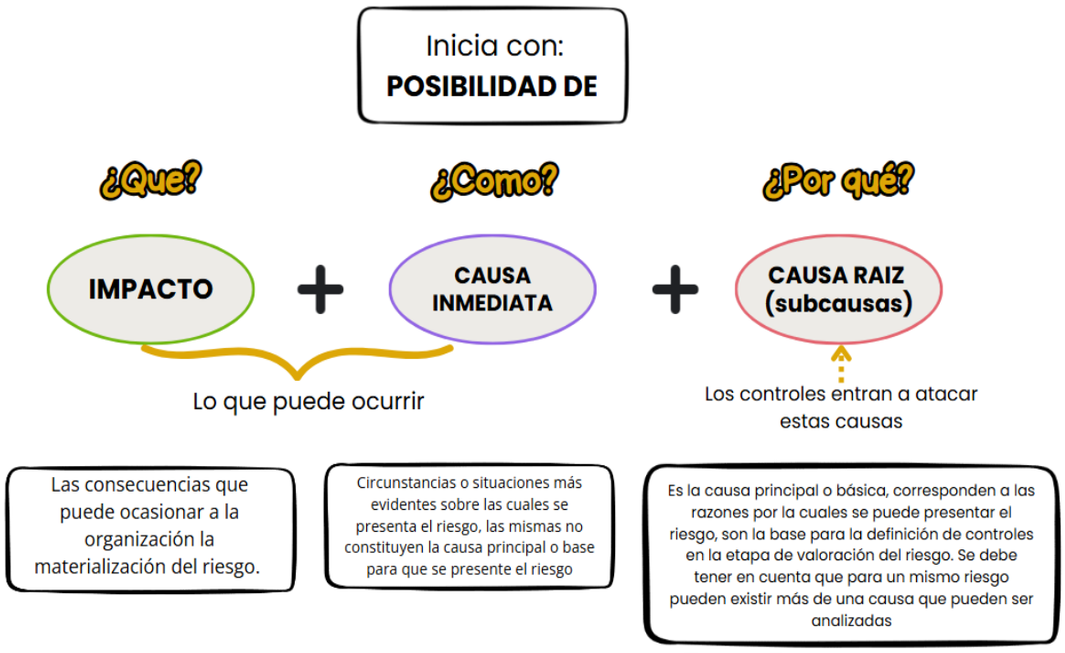
Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Accesos no autorizados a información de la entidad
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento Externo	Situaciones externas que afectan la entidad	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Guía para la administración del riesgo y el diseño de controles

en entidades Públicas 2022. Versión 6

6.2.1.4 Descripción del Riesgo. Debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos:

Figura 3. Estructura propuesta para la redacción del riesgo



Esta estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas raíz, esta información es esencial para la definición de controles en la etapa de valoración del riesgo.

Algunas premisas para una adecuada redacción del riesgo:

- No describir como riesgos omisiones ni desviaciones del control
- No describir causas como riesgos
- No describir riesgos como la negación de un control
- No existen riesgos transversales, lo que pueden existir son causas transversales.

Ejemplo: perdida de expedientes

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

6.2.1.5 Clasificación del Riesgo**.** Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 6. Clasificación y factores de Riesgos

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

6.3 ANÁLISIS DE RIESGO INHERENTE

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

El Riesgo Inherente es el resultado de combinar la probabilidad con el impacto, permite determinar el nivel de riesgo inherente dentro de unas escalas de severidad.

6.3.1 Determinar la probabilidad**.** Se entiende como la posibilidad de ocurrencia del riesgo. Es decir, la probabilidad inherente será el **número de veces que se pasa por el punto de riesgo en el periodo de 1 año** y se basa en la **exposición al riesgo** del proceso o actividad que se esté analizando.

De este modo, **la probabilidad analiza la frecuencia con la que se realiza la actividad, y no se basa en eventos**. En la tabla 7 se establecen los criterios para definir el nivel de probabilidad.

Tabla 7. Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

6.3.2 Determinar el impacto**.** Son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. La tabla 8 de criterios, definen los impactos económicos y reputacionales como las variables principales.

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 insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Tabla 8. Criterios para definir el nivel de impacto

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

Ejemplo para la aplicación de la tabla 6 de probabilidad y la tabla 7 de impacto:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

→ La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es

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

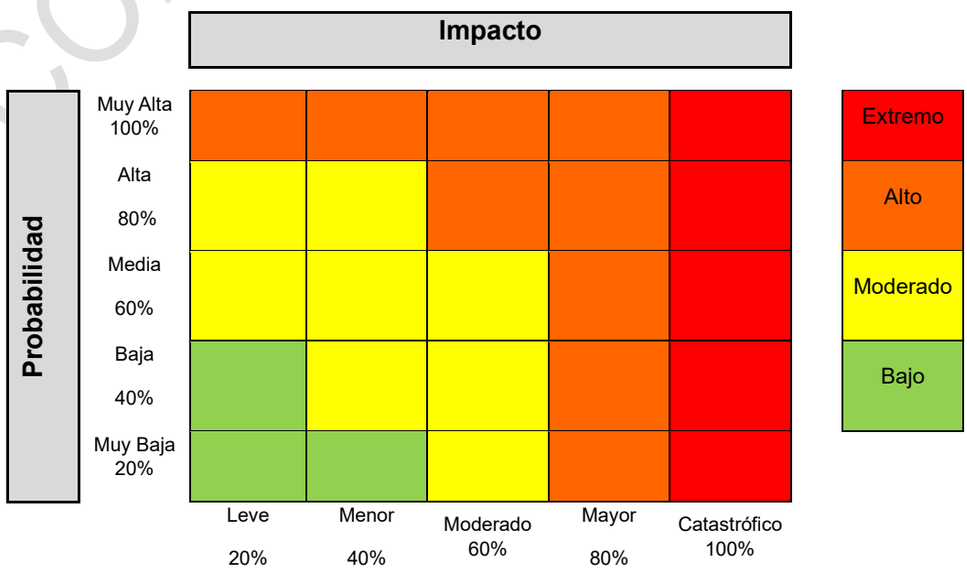
→ La afectación económica se calcula en 500SMLMV, el impacto del riesgo es

De acuerdo con la aplicación de las tablas 6 y 7 para el ejemplo la **Probabilidad inherente =** media 60%, y el **Impacto inherente:** mayor 80%.

6.3.3 Análisis de Severidad. A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver figura 5).

Figura 4. Matriz de calor (niveles de severidad del riesgo)



Continuando con el ejemplo donde la **Probabilidad inherente =** media 60%, y el **Impacto inherente:** mayor 80%, se aplica la Matriz de Calor, se tiene:

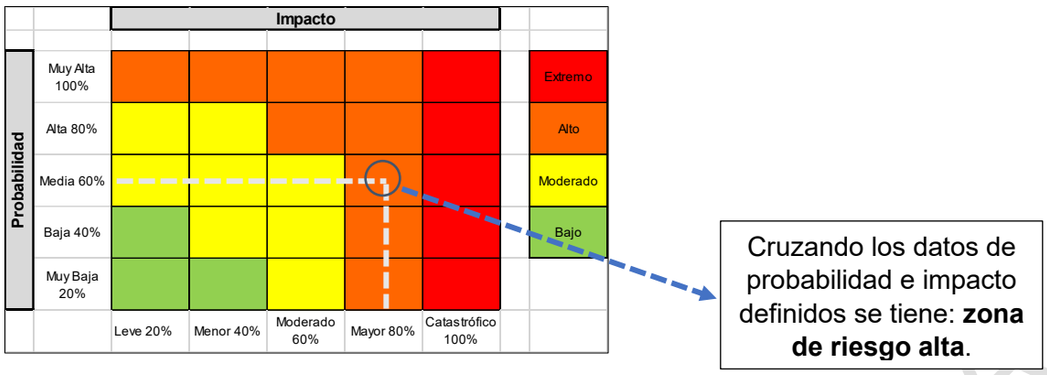


Tabla 9. Matriz Identificación del Riesgo y Análisis del Riesgo Inherente

Identificación del riesgo							Análisis del riesgo inherente					
Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente
1												
2												

6.4 DISEÑO Y ANÁLISIS DE CONTROLES

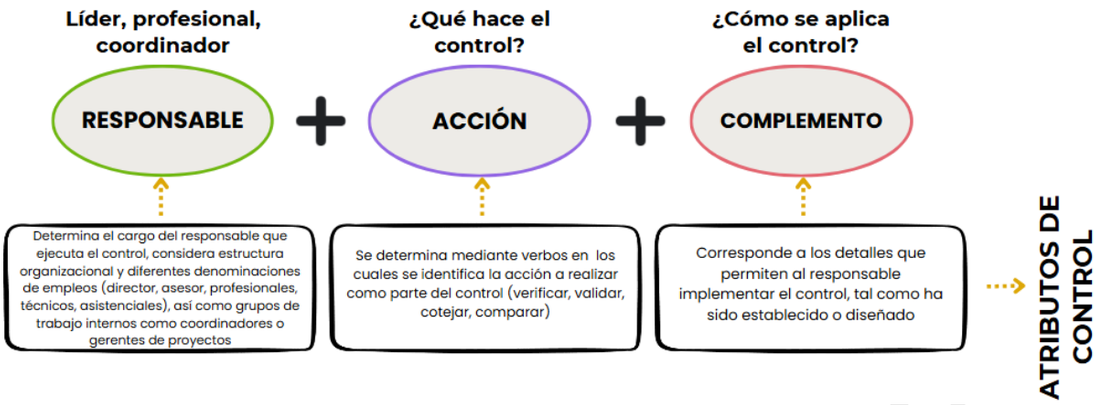
Se establece la siguiente ruta para la identificación o definición de controles, con base en atributos de diseño que garanticen su cumplimiento por el responsable y permitan su correspondiente valoración

¿Que son las actividades de control?: Son las acciones a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la alta dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos de la entidad.

Premisas para el diseño y análisis de controles:

- Una política por sí sola no es un control
- La actividad de control debe por si sola mitigar o tratar la causa del riesgo y ejecutarse como parte del día a día de las operaciones
- Los controles se despliegan a través de los procedimientos documentados, sistemas de información u otras herramientas que permitan su trazabilidad.

6.4.1 Estructura para la descripción del control**:** para un adecuado diseño del control se propone una estructura para la redacción del control que agrupa los atributos necesarios para garantizar su implementación por parte del responsable.



6.4.2 Tipologías de Controles.

Con el fin de establecer la tipología de los controles para su posterior validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo.

6.4.3 Valoración de Controles**:** La tabla aplicable para la valoración de controles que se muestra a continuación, determina la forma como se califica los atributos o características de eficiencia, todos los demás atributos informativos o de formalización del control, no se aplica valoración, pero son esenciales para garantizar su efectividad.

Tabla 10. Valoración de controles

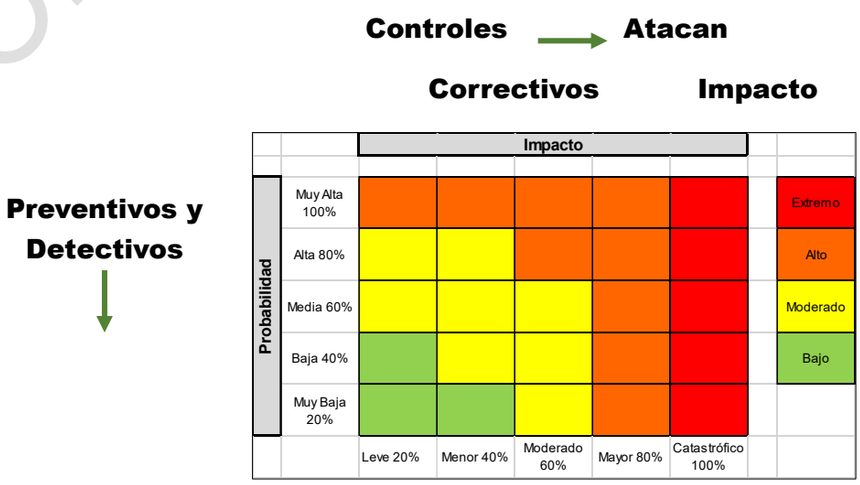
Características de Eficiencia			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%

		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%

	Formalización del Control	
Atributos informativos	Documentación	Procedimientos
		Otros esquemas
	Frecuencia (adecuada para detectar o prevenir el riesgo)	Continua
		Aleatoria
	Evidencia (trazabilidad de la ejecución)	Con registro físico manual
		Con registro electrónico
	Ejecución (fuentes de información que sean confiables)	Interna
		Externa
		Mixta

6.4.4 Aplicación de Controles en la matriz de severidad**.** Teniendo en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor, a continuación, se muestra cual es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Figura 5. Movimiento en la matriz de calor acorde con el tipo de control



6.5 VALORACIÓN DE RIESGO RESIDUAL.

A continuación, se desarrollan los pasos necesarios para aplicar la efectividad de los controles al riesgo inherente.

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

Dependiendo del nivel de severidad en que se ubique el riesgo residual, la entidad podrá priorizar la atención de estos, así como definir su tratamiento y las acciones a seguir.

Ejemplo:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de afectación económica por condena en contra de la entidad debido a errores en la adjudicación del proceso contractual	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2%**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Nota: La entidad deberá implementar en el marco de su gestión del riesgo una política de reducción máximo del 50%, para evitar que un solo control baje mucho el nivel del riesgo (ejemplo: Control = preventivo (49%) + automático (49%) = 98%).

Tabla 11. Matriz Valoración del Riesgo

Paso 4. Valoración del Riesgo

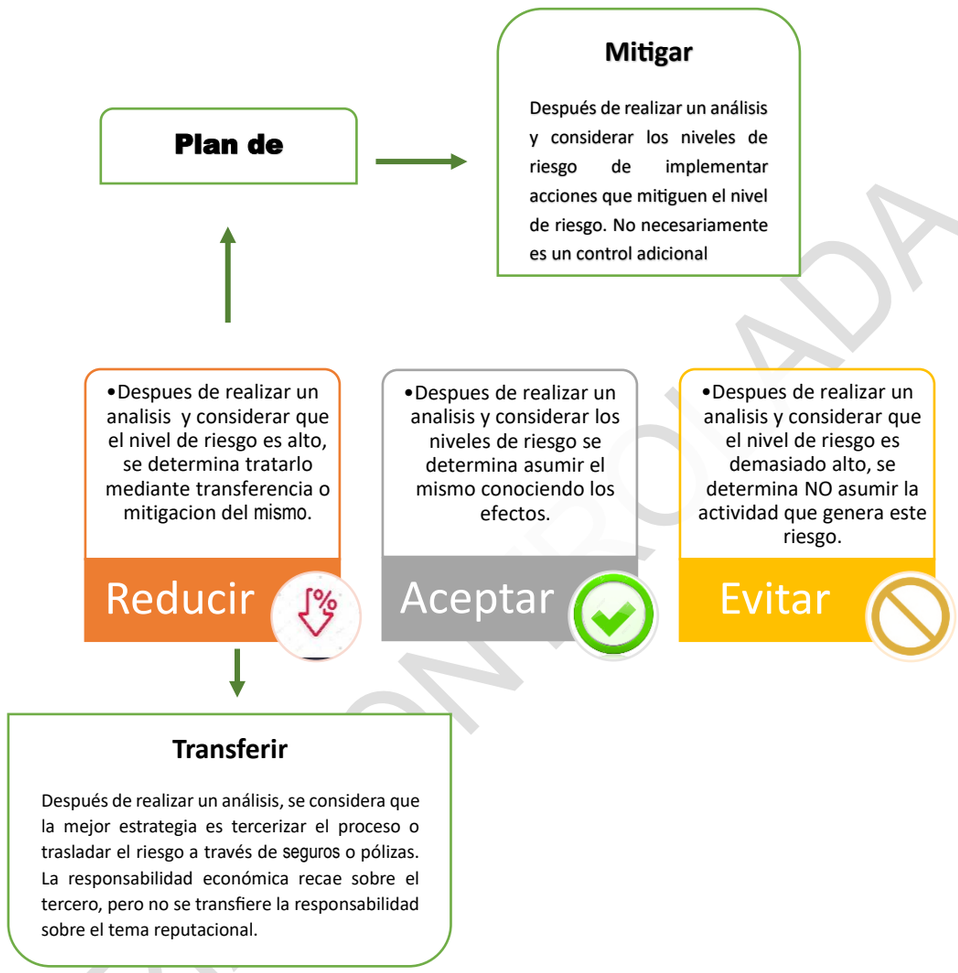
Evaluación del riesgo - Valoración de los controles											**Evaluación del riesgo - Nivel del riesgo residual**					
			Atributos													
No. Control	**Descripción del Control**	**Afectación**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Ejecución**	**Probabilidad Residual**	**Probabilidad Residual Final %**	**Impacto Residual Final**	**%**	**Zona de Riesgo Final**	**Tratamiento**
1															
2															

- Estrategias para combatir el riesgo**.** Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo

residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la figura 7 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Figura 6. Estrategias para combatir el riesgo



Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) entregable, iii) fecha de inicio y iv) fecha de terminación.

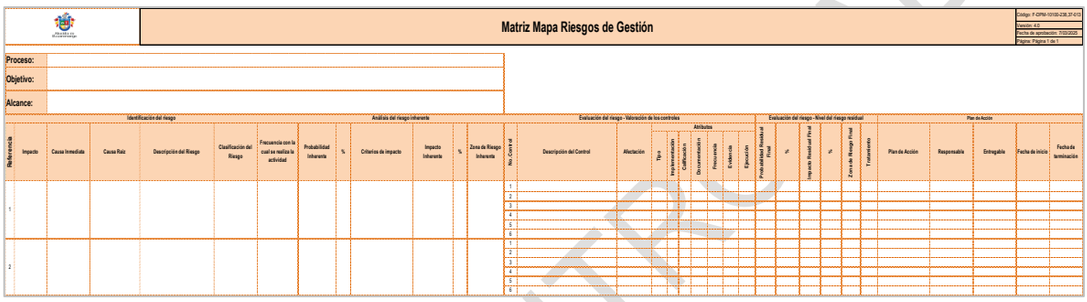
Tabla 12. Plan de acción (para la opción de tratamiento reducir)

Plan de Acción

Plan de Acción	**Responsable**	**Entregable**	**Fecha de inicio**	**Fecha de terminación**

Como producto de la aplicación de la metodología se contará con la **MATRIZ MAPA RIESGOS DE GESTIÓN,** código F-DPM-1210-238,37-013, en la cual se consolida los riesgos identificados por proceso.

Tabla 13. Matriz Mapa Riesgos de Gestión


Matriz Mapa Riesgos de Gestión

Proceso:
Objetivo:
Alcance:

Identificación del riesgo						Análisis del riesgo inherente					Evaluación del riesgo - Valoración de los controles								Evaluación del riesgo - Nivel del riesgo residual					Plan de Acción				
Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de Impacto	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Atributos: Tipo	Atributos: Implementación	Atributos: Calificación	Atributos: Documentación	Atributos: Frecuencia	Atributos: Evidencia	Atributos: Disposición	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Entregable	Fecha de inicio	Fecha de terminación
1													1																				
													2																				
													3																				
													4																				
													5																				
													6																				
2													1																				
													2																				
													3																				
													4																				
													5																				
													6																				

GESTIÓN PREVENTIVA DE RIESGOS FISCALES

7.1 CONTROL FISCAL INTERNO Y PREVENCIÓN DEL RIESGO FISCAL

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

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

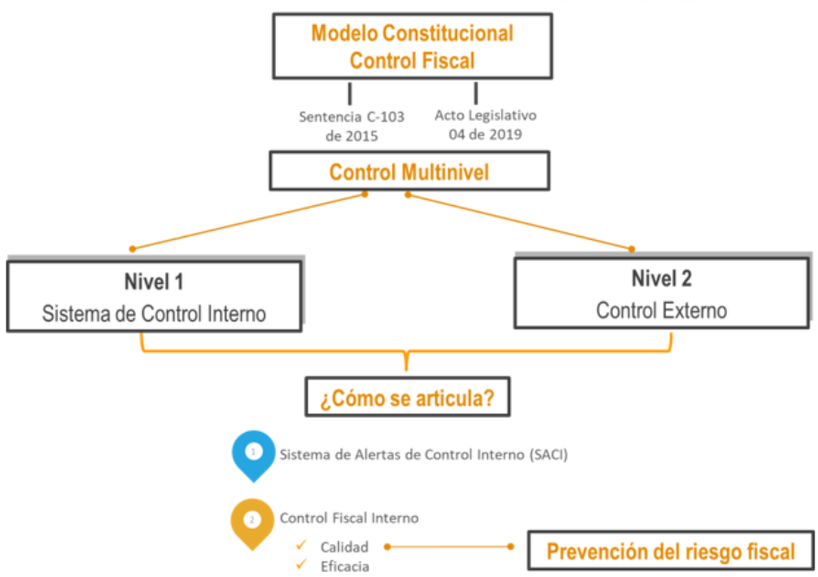
De acuerdo con lo anterior, el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el Sistema de Control Interno, con lo cual surgen los siguientes conceptos:

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

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

El Sistema de Control Interno es fundamental para el logro de resultados a través de la prevención de responsabilidades, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labor es de cobro, entre otros).

Figura 7. Articulación modelo constitucional control fiscal y Sistema de Control Interno



Fuente: Función Pública, 2022

7.2 METODOLOGÍA PARA LA FORMULACIÓN DEL MAPA DE RIESGOS FISCALES

Se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, para el resultado de la gestión de la entidad, la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros).

7.2.1 Identificación y Descripción del Riesgo Fiscal. Es necesario establecer los puntos de riesgo fiscal y las circunstancias inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas[1].

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

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

Para identificar los puntos de riesgo y las circunstancias inmediatas, se debe realizar mesas de trabajo con los lideres de proceso y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor en la identificación de puntos de riesgo fiscal y circunstancias inmediatas. Para estas mesas de trabajo, se puede usar las siguientes preguntas orientadoras:

Tabla 14. Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo 3. Términos y conceptos).
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno – SACI.

1 Artículo 3 Ley 610 de 2000.

	1. Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. 2. Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de los planes de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno de Gestión. 3. Los fallos con responsabilidad fiscal en firme son información pública. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. 4. La consolidación de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI- es una labor de la segunda línea de defensa (Secretaría de Planeación) con la asesoría de la Oficina de Control Interno de Gestión.
Circunstancias inmediatas	En este ejercicio autocritico, realista y objetivo, identificar ¿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 de Gestión, en los últimos 3 años? 1. Luego del análisis de las causas, la entidad concluye si la causa del hallazgo es la identificada por el órgano de control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del “¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” (anexo1), son aplicables a la entidad?

Fuente: Función Pública, 2022.

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

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

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- ✓ Los riesgos de daño antijurídico - riesgo de pago de condenas y conciliaciones.
- ✓ Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo 3. Términos y conceptos).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública (consultar definiciones en el capítulo 3. Términos y conceptos).

7.2.1.3 Identificación de la causa raíz o potencial hecho generador. La causa raíz es el evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

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

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

Cabe aclarar que se debe separar el hecho que ocasiona el daño (hecho generador - causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador – causa -, y otro es el daño – efecto - (Contraloría General de la República, 2021)[2].

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

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

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

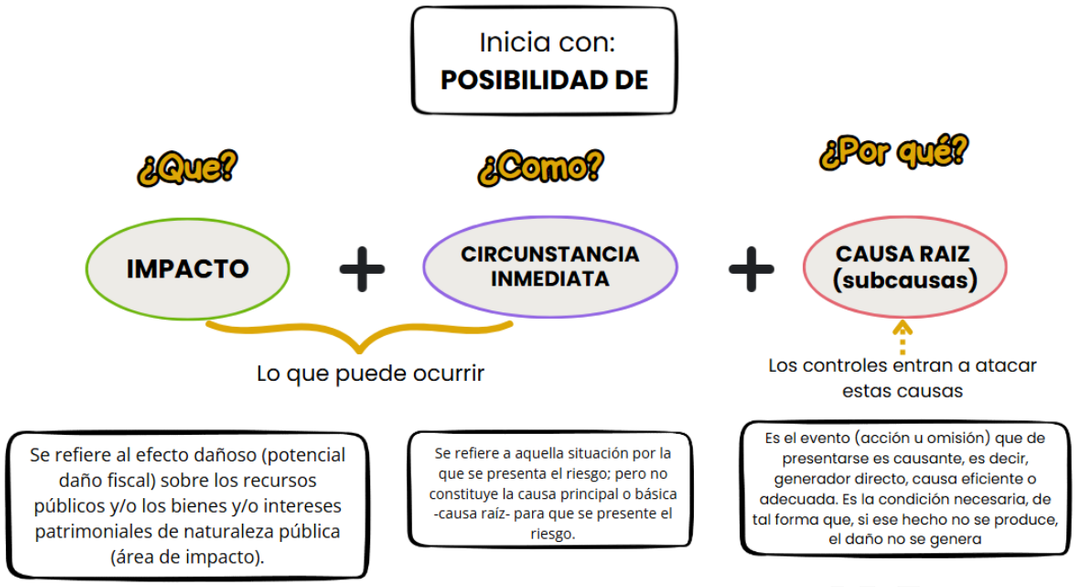
Conclusión: *El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.*

7.2.1.4 Descripción del Riesgo Fiscal. La estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos y algunos ejemplos de riesgos fiscales identificados en el anexo 1. Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.

Para redactar un riesgo fiscal se debe tener en cuenta:

2 Concepto CGR- OJ- 115 - 2021 de la Contraloría General de la República, pág. 13

Figura 8. Estructura propuesta para la redacción del riesgo fiscal

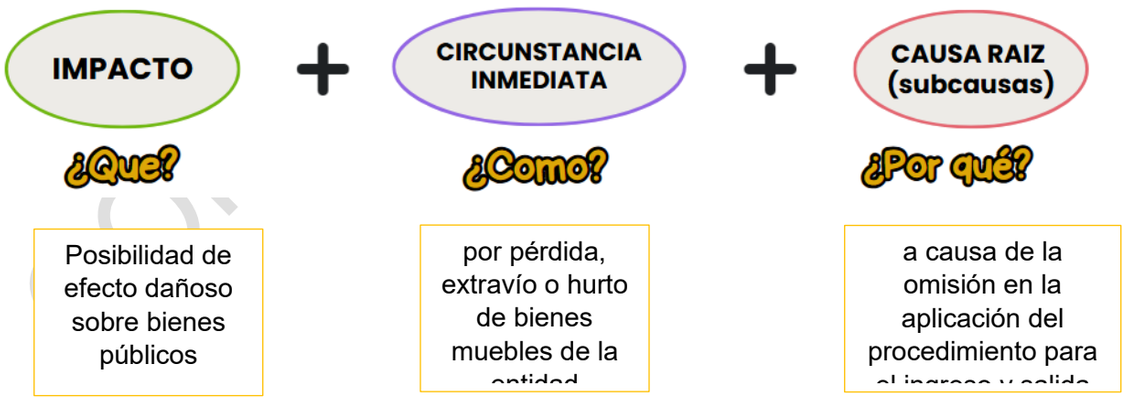


Ejemplo:

Proceso: *Gestión de Recursos*

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

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



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

Tabla 15. Ejemplos según el objeto sobre el cual recae el efecto dañoso

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

Fuente: Función Pública, 2022

7.3 ANALISIS DE RIESGO INHERENTE

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

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

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

Tabla 16. Criterios para definir el nivel de probabilidad en riesgos fiscales

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

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

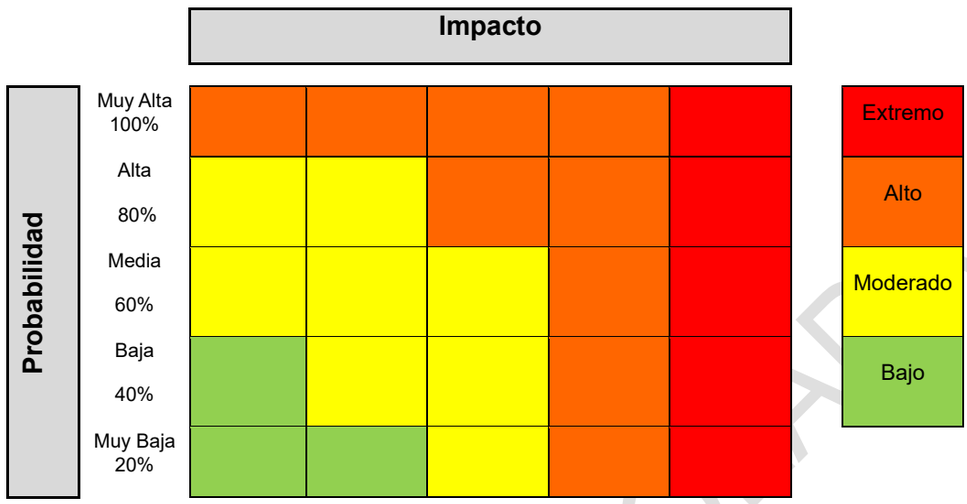
Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos. Existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la siguiente tabla:

Tabla 17. Criterios para definir el nivel de impacto en riesgos fiscales

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

7.3.3 Análisis de severidad**.** A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad, para lo cual se aplica la siguiente matriz:

Figura 9. Matriz de calor (niveles de severidad del riesgo fiscal)



Ejemplo (continuación):

Proceso: *Gestión de recursos*

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

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

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

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

Probabilidad: *Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varían en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.*

Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

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

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

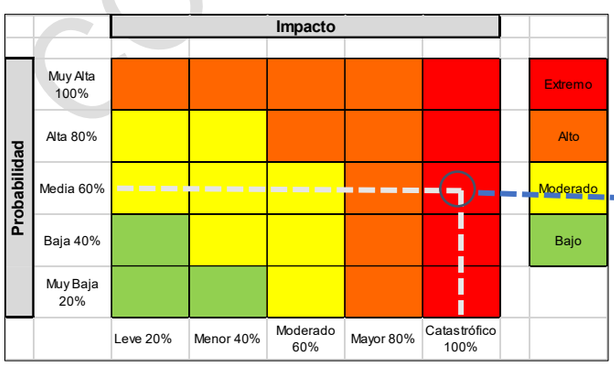
En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de $2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico.

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

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

De acuerdo con la aplicación de las tablas 15 y 16 para el ejemplo la **Probabilidad inherente =** media 60%, y el **Impacto inherente:** catastrófico 100%.

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



Cruzando los datos de probabilidad e impacto definidos se tiene: **zona de riesgo extrema**

7.4 DISEÑO Y ANALISIS DE CONTROLES

Las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

7.4.1 Estructura para la descripción del control. Se propone la siguiente estructura que facilitará más adelante entender su tipología y otros atributos para su valoración:

- ✓ **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- ✓ **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- ✓ **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto

7.4.2 Tipologías de controles**:** Con el fin de establecer la tipología de los controles para su posterior validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo.

7.4.3 Valoración de Controles

Tabla 18. Valoración de controles

Características de Eficiencia			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	10%

		riesgo, tienen un costo en su implementación.	
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	Formalización del Control		
	Documentación	Procedimientos	
		Otros esquemas	
	Frecuencia (adecuada para detectar o prevenir el riesgo)	Continua	
		Aleatoria	
	Evidencia (trazabilidad de la ejecución)	Con registro físico manual	
		Con registro electrónico	
	Ejecución (fuentes de información que sean confiables)	Interna	
		Externa	
		Mixta	

Ejemplo (continuación):

Proceso: *Gestión de recursos*

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

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

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

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

Probabilidad Inherente: *Media 60%*

Impacto Inherente*: Catastrófico 100%*

Zona de riesgo: *Extrema*

Controles Identificados en el ejemplo:

- ✓ **Control 1 Preventivo:** El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.
- ✓ **Control 2 Detectivo:** El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.
- ✓ **Control 3 Correctivo:** El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador

Tabla 19. Ejemplo aplicación valoración de controles de riesgos fiscales

Control 1	**Criterios de efectividad**			**Peso**
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 1 = 40%			
Control 2	**Criterios de efectividad**			**Peso**
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 2 = 30%			
Control 3	**Criterios de efectividad**			**Peso**
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	X	10%
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 3 = 25%			

En la matriz de calor se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y su respectiva valoración, a fin de determinar el riesgo residual.

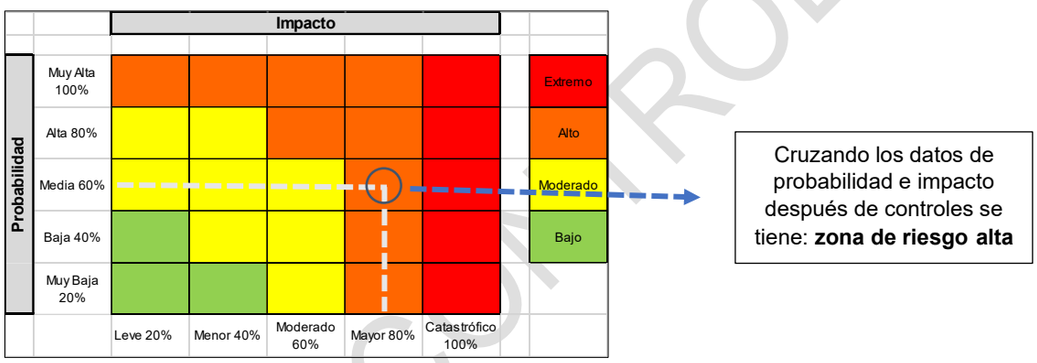
7.5 VALORACIÓN DEL RIESGO RESIDUAL

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

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

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

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



LINEAMIENTOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN (PROCESO DE TRANSICIÓN A RIESGOS INTEGRIDAD PÚBLICA)

En materia de riesgos asociados a posibles actos de corrupción, se consideran los siguientes aspectos:

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

8.1 IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN

8.1.1 Procesos, procedimientos o actividades susceptibles de riesgos de corrupción**.** A manera de ilustración a continuación se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos:

Tabla 20. Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

Direccionamiento estratégico (alta dirección)	● Concentración de autoridad o exceso de poder. Extralimitación de funciones. ● Ausencia de canales de comunicación. ● Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	● Inclusión de gastos no autorizados. ● Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. ● Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. ● Inexistencia de archivos contables. ● Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	● Estudios previos o de factibilidad deficientes. ● Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). ● Pliegos de condiciones hechos a la medida de una firma en particular. ● Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). ● Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. ● Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. ● Urgencia manifiesta inexistente. ● Concentrar las labores de supervisión en poco personal. ● Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	● Ausencia o debilidad de medidas y/o políticas de conflictos de interés. ● Concentración de información de determinadas actividades o procesos en una persona. ● Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. ● Ocultar la información considerada pública para los usuarios. ● Ausencia o debilidad de canales de comunicación
De Investigación y Sanción	● Ausencia o debilidad de medidas y/o políticas de conflictos de interés. ● Concentración de información de determinadas actividades o procesos en una persona. ● Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración.

	● Ocultar la información considerada pública para los usuarios. ● Ausencia o debilidad de canales de comunicación
De trámites y/o servicios internos y externos	● Cobros asociados al trámite. ● Influencia de tramitadores. ● Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	● Falta de procedimientos claros para el trámite ● Imposibilitar el otorgamiento de una licencia o permiso. ● Tráfico de influencias: (amiguismo, persona influyente).

Figura 10. Descripción del riesgo de corrupción

RIESGO DE CORRUPCIÓN

Definición de Riesgo de corrupción:

Riesgo de Corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

"Esto aplica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes No. 167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición así:

▪ ACCIÓN U OMISION

▪ USO DEL PODER

▪ DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO

▪ EL BENEFICIO PRIVADO

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción porque incorpora cada uno de los componentes de su definición.

Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

Tabla 21. Matriz para la definición del riesgo de corrupción

Matriz definición del riesgo de corrupción				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo publico**	**Beneficio privado**
Riesgo 1	**X**	**X**	**X**	**X**

8.2 ANALISIS DEL RIESGO INHERENTE

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

8.2.1 Determinación de la probabilidad**.** Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad:

FRECUENCIA	FACTIBILIDAD
Bajo el criterio de FRECUENCIA se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.	Bajo el criterio de FACTIBILIDAD se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Para su determinación se utiliza la tabla de criterios para calificar la probabilidad.

Tabla 22. Criterios para calificar la probabilidad en riesgos de corrupción

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

En caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

Tabla 23. Matriz de priorización de probabilidad

No.	Riesgo	Probabilidad por matriz de priorización	Promedio	Participante 1	Participante 2	Participante 3	Participante 4	Participante 5…
R1								
R2								
R3								

8.2.2 Determinación del impacto**.** Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos.

Para establecer estos niveles de impacto se deberán aplicar las siguientes preguntas frente a cada riesgo identificado:

Tabla 24. Criterios para calificar el impacto en riesgos de corrupción

No.	PREGUNTA: Si el riesgo de corrupción se materializa podría…	Respuesta SI	Respuesta NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de la misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicio o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los entes de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinario?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	**¿Ocasionar lesiones físicas o pérdidas de vidas humanas?**		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado		**10**	
Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor			
Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		

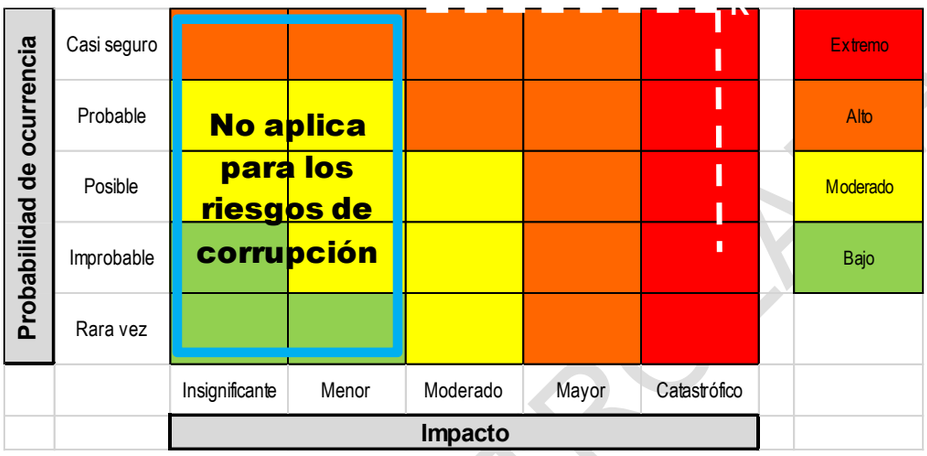
Fuente: Secretaría de Transparencia de la Presidencia de la República.

Observación: Si la respuesta a la pregunta 16 es afirmativa, automáticamente el impacto será **catastrófico.**

8.2.3 Análisis de severidad**.** El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Mapa de calor. Se toma la calificación de probabilidad resultante de la tabla "Matriz de priorización de probabilidad", y la calificación de impacto, ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel del riesgo, así se podrá determinar el riesgo inherente.

Figura 11. Matriz de calor para riesgos de corrupción



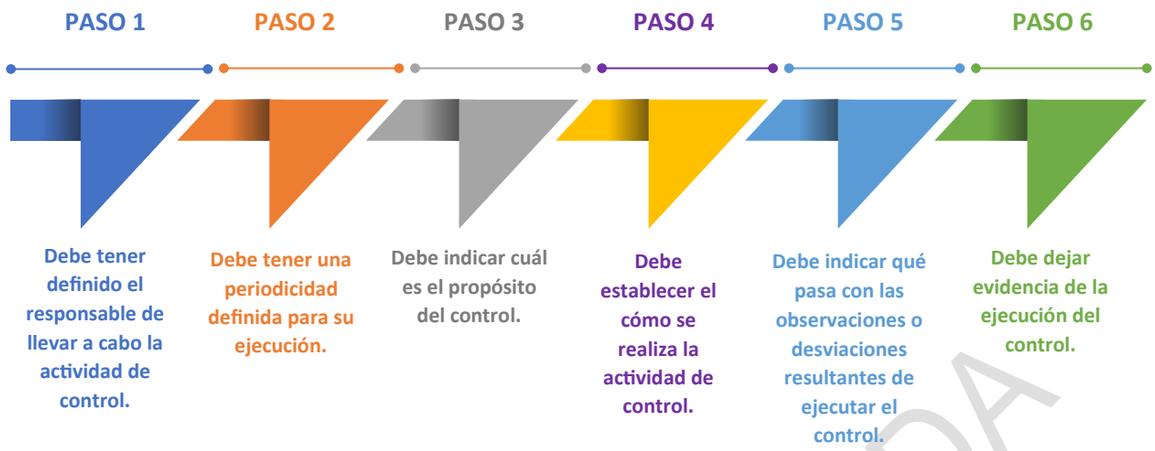
8.3 DISEÑO Y ANALISIS DE CONTROLES

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

- Para cada causa debe existir un control.
- Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).
- Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

8.3.1 Estructura para descripción del Control**.** Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo, se deben considerar desde la redacción del mismo, las siguientes variables para la evaluación del diseño del control:

Figura 12. Pasos para diseñar un control



Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

El análisis y evaluación del diseño del control se realiza de acuerdo con las seis (6) variables establecidas:

Tabla 25. Análisis y evaluación de los controles para la mitigación de los riesgos.

CRITERIO DE EVALUACIÓN	ASPECTOS A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No asignado	0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No Confiable	0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente.	0
		Completa	10

6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Incompleta	5
		No existe	0

8.3.1.1 Resultados de la evaluación del diseño del control. El resultado de cada variable de diseño (tabla 25), a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

Del mismo modo, aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo, y asegurarse por parte de la primera línea de defensa que el control se ejecute.

Tabla 26. Solidez de controles

Peso del diseño de cada control	Peso de la ejecución del control	Solidez individual de cada control	Debe establecer acciones para fortalecer el control SI / NO
Fuerte Calificación entre 96 y 100	fuerte (se ejecuta de manera consistente).	fuerte + fuerte = fuerte	NO
	moderado (se ejecuta algunas veces)	fuerte + moderado = moderado	SI
	débil (no se ejecuta)	fuerte + débil = débil	SI
Moderado Calificación entre 86 y 95	El control se ejecuta algunas veces por parte del responsable	moderado	SI
Débil Calificación entre 0 y 85	El control no se ejecuta por parte del responsable	débil	SI

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un **Plan de acción** que permita tener un control o controles bien diseñados.

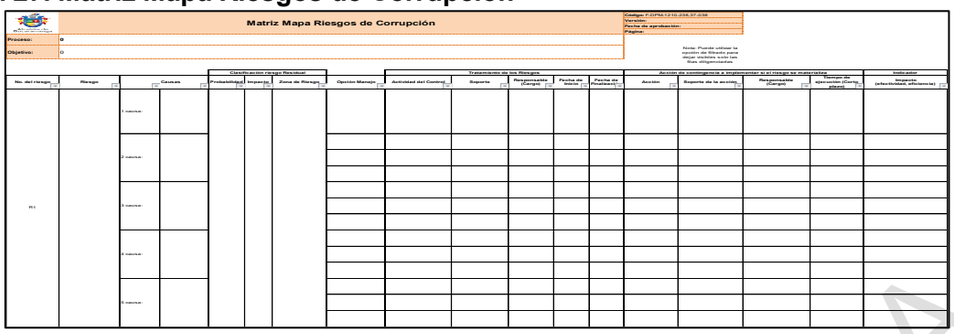
8.3.1.2 Plan de Acción. Una vez establecida la opción de manejo del riesgo se relacionan las actividades de control, el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer, cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso.

Por último, se formularán los indicadores que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades del control, siempre y cuando conduzcan a la toma de decisiones (por riesgo identificado en los procesos).

Para la construcción del Mapa de Riesgos de Corrupción incluido en el Programa de Transparencia y Ética Pública – PTEP se realizará teniendo en cuenta la **Matriz Mapa Riesgos de Corrupción F-DPM-1210-238,37-036** de acuerdo con los lineamientos y matriz suministrada por la Secretaría de Transparencia de la Presidencia de la República.

Tabla 27. Matriz Mapa Riesgos de Corrupción



Matriz Mapa Riesgos de Corrupción

Proceso: 0

Objetivo: 0

Nombre del riesgo | Riesgo | Causas | Clasificación riesgo Residual: Probabilidad, Impacto, Zona de Riesgo | Opción Manejo | Tratamiento de los Riesgos: Actividad del Control, Soporte, Responsable (Cargo), Fecha de Inicio, Fecha de Finalización | Acciones de contingencia a implementar si el riesgo se materializa: Acción, Soporte de la acción, Responsable (Cargo), Tiempo de ejecución (Días, meses, años) | Indicador: Impacto (eficacia/eficiencia)

R1

1 causa

2 causa

3 causa

4 causa

5 causa

NIVELES DE ACEPTACIÓN DE LOS RIESGOS DE GESTIÓN Y DE CORRUPCIÓN IDENTIFICADOS

La Política de Administración de Riesgos establece las opciones para tratar y manejar los riesgos basada en la valoración de estos, a partir de los criterios ERCA: Evitar, Reducir, Compartir y Asumir.

Por tanto, la entidad establece los siguientes niveles de aceptación y periodicidad de seguimiento a los riesgos identificados (Ver tabla 28):

Tabla 28. Nivel de Aceptación del Riesgo

NIVEL DE ACEPTACIÓN DEL RIESGO
De acuerdo con las responsabilidades establecidas en la presente política, las siguientes acciones estarán a cargo de cada proceso: 1) Cuando al medir la probabilidad e impacto de un riesgo residual de Proceso, éste quede catalogado en **nivel BAJO**, se **ASUMIRÁ el riesgo** y se administrará por medio de las actividades propias del Plan o Proceso asociado y su control y registro de avance se realizará en el documento establecido en el Sistema Integrado de Gestión de Calidad - SIGC. 2) Cuando el nivel del riesgo sea **MODERADO**, se establecerán acciones de Control Preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento **BIMESTRAL** (cada dos meses) y se registrará sus avances en el documento establecido en el SIGC. 3) Cuando el nivel del riesgo residual queda ubicado en la zona de **riesgo ALTA**, se deberá incluir el riesgo en el *Mapa de Riesgos* y se establecerán acciones para abordar los riesgos y las oportunidades que permitan **EVITAR** la materialización de este. La Administración de estos riesgos será con periodicidad **al menos MENSUAL** y su adecuado control se registrará sus avances en el documento establecido en el SIGC. 4) Si el Nivel del riesgo residual se ubica en la zona de **riesgo EXTREMA**, se incluirá el riesgo en el *Mapa de Riesgo* y se establecerán acciones correctivas y preventivas para abordar los riesgos y las oportunidades que permitan **EVITAR** la

materialización del riesgo. La Administración de estos riesgos será con periodicidad **mínima MENSUAL** y su adecuado control se registrará sus avances en el documento establecido en el SIGC.

NOTA: Los riesgos de corrupción no admiten aceptación del riesgo, siempre debe conducir a un tratamiento.

De igual manera, cuando en el seguimiento periódico que realicen los líderes de proceso a sus respectivos mapas de riesgo se prevea la **materialización del riesgo**, se establecerán **acciones para abordar riesgos** de manera inmediata a través de un Plan de Mejoramiento Institucional, con acciones diferentes a las planificadas inicialmente y se analizará la pertinencia de los controles previamente definidos, asegurando la continuidad del servicio o el restablecimiento de este.

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

9.1 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

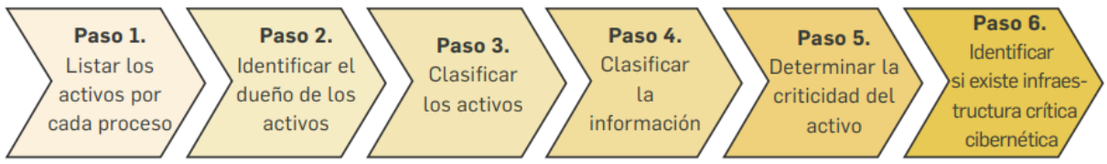
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información, son activos de información los elementos que utiliza la entidad para funcionar en el entorno digital y que necesitan ser protegidos, tales como: documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados.

Al identificar los activos también es necesario identificar a sus propietarios, es decir, la persona o unidad organizativa responsable de éste.

De acuerdo con lo anterior, se debe determinar qué es lo más importante que la Administración Municipal y sus procesos poseen (bases de datos, archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios), que permita saber qué es lo que se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Teniendo en cuenta que la Seguridad de la Información debe aplicarse a la totalidad de la operatividad de la entidad, los activos que hacen parte de procesos críticos o misionales estarán clasificados como de mayor importancia y, de acuerdo con el proceso, los demás activos tendrán asignado un nivel de criticidad en cuanto a la información que contienen o gestionan.

La identificación y valoración de activos debe ser realizada por los Líderes de Proceso (primera línea de defensa) en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de Seguridad de la información de la Administración Municipal, con los siguientes pasos:



Paso 1. Listar los activos por cada proceso. En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Paso 2. Identificar el dueño de los activos. Cada uno de los activos identificados deberá tener un propietario designado, Si un activo no posee un propietario, nadie se hará responsable ni lo protegerá debidamente.

Paso 3. Clasificar los activos. Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red, entre otros.

Paso 4. Clasificar la información. Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía No.5 de Gestión y Clasificación de Activos, el Dominio 8 (Gestión de Activos) del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.

Paso 5. Determinar la criticidad del activo. La entidad debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno para posteriormente, durante el análisis de riesgos, tener presente esta criticidad y así hacer una valoración adecuada de cada caso.

En este paso se deben definir las escalas de criticidad (ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas. Identificar y reportar a las instancias y autoridades respectivas en el Gobierno nacional si poseen Infraestructuras Críticas Cibernéticas - ICC. Se debe tener en cuenta que el sector Gobierno, al cual pertenece la Alcaldía de Bucaramanga, tiene asignada la escala de valoración de impacto ALTO.

9.2 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

La Alcaldía de Bucaramanga designará al responsable de Seguridad de la información, quien deberá cumplir las siguientes responsabilidades respecto a la gestión del riesgo de seguridad de la información:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).

- Asesorar y acompañar a los líderes de proceso (primera línea de defensa) en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Realizar seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la Alta Dirección (línea estratégica) sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información

9.3 IDENTIFICACIÓN DE LOS RIESGOS INHERENTES DE SEGURIDAD DE LA INFORMACIÓN

Se definen tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Los riesgos de seguridad de la información forman parte de los riesgos de proceso, y por tanto se contempla dentro de la metodología descrita en la presente Política de Administración de Riesgos, aplicable a todos los procesos de la Administración Municipal, teniendo en cuenta, además, aspectos descritos en el Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad digital en Entidades Públicas - Guía riesgos 2018.

Los ítems anteriormente mencionados se encuentran alineados con los criterios estipulados en la Política de Seguridad y Privacidad de la Información publicada en la Resolución-0489 del 29 de diciembre de 2017, que es el marco normativo que ha adoptado el municipio para gestionar la toma de decisiones para la Seguridad de Información a través de la articulación de los Sistemas de Gestión de la Administración, implementando políticas, controles y procedimientos que permitan de manera oportuna la atención de riesgos de Seguridad de la Información, así como la buena gestión de la información en el Municipio.

9.4 ESTIMACIÓN DEL RIESGO

Una vez que se han identificado los riesgos, es necesario evaluar el impacto para cada combinación de amenazas y vulnerabilidades de un activo de información específico, en caso de que ello se produzca.

9.4.1 Probabilidad. La posibilidad de ocurrencia del riesgo, representa el número de veces que pasa por el punto del riesgo en un determinado tiempo o que pueda presentarse dicho riesgo. Siguiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, se toma para este criterio como línea tiempo el periodo de un (1) año con los valores recomendados.

Es importante destacar que la siguiente tabla define la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo de información en cuestión.

Tabla 29. Criterios para definir el nivel de probabilidad Riesgos en activos de información

	Frecuencia de la Actividad	Probabilidad	Relación – Controles
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%	Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección. En el futuro no se esperan incidentes nuevos.
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%	Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección. Es posible la ocurrencia de nuevos incidentes, pero no muy probable.
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%	Los controles de seguridad existentes son bajos o ineficaces. Existe una gran probabilidad de que haya incidentes así en el futuro.
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%	

Tomado y adaptado de Guía para la administración de riesgo y diseño de controles en entidades públicas
Diciembre 2020 – Versión 5

9.4.2 Impacto: Hace referencia a las consecuencias que puede ocasionar a la Alcaldía de Bucaramanga la materialización del riesgo; se refiere a la magnitud de sus efectos. De igual forma y tomando como base la Guía para la administración de riesgo y diseño de controles en entidades públicas y alineándose con estrategia del municipio, se han asumido los criterios y niveles de afectación de acuerdo con dicha tabla:

Tabla 30. Criterios para definir el nivel de Impacto en Riesgos de activos de información

	Afectación económica	Reputacional	Relación – Confidencialidad/Integridad/Disponibilidad
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la entidad.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores	
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la entidad.
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.	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país	

Tomado y adaptado de Guía para la administración de riesgo y diseño de controles en entidades públicas
Diciembre 2020 – Versión 5

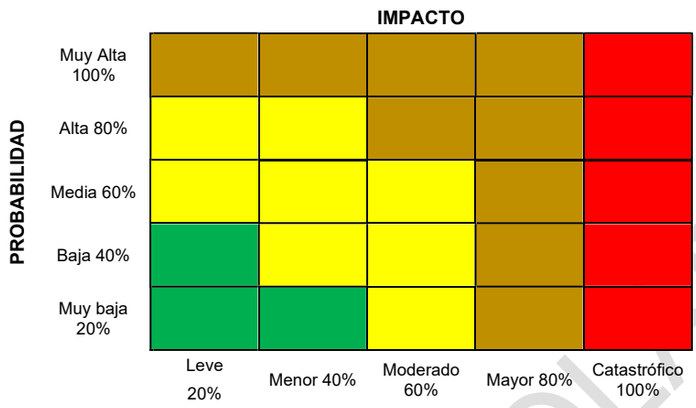
9.5 DETERMINACIÓN DEL RIESGO INHERENTE Y RESIDUAL

De acuerdo plan de tratamiento de riesgos de seguridad digital en el cual se especifica que la exposición al riesgo es la ponderación de la probabilidad e impacto (*Riesgo = Probabilidad * Impacto*).

En la siguiente tabla se muestra la matriz de riesgo, instrumento que muestra las zonas de riesgo y que facilita el análisis gráfico.

Esta herramienta permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados (zona de riesgo **BAJO**, **MODERADO**, **ALTO** o **EXTREMO**) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Figura 13. Matriz de Calor Riesgos de Seguridad de la Información



Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional para la Alcaldía – adaptado del DAFP.

Para la construcción del Mapa de Riesgos de Seguridad de la Información se realizará teniendo en cuenta la **Matriz Mapa Riesgos de Seguridad de la Información F-TIC-1400-238,37-047** de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC y la Guía para la administración de riesgo y diseño de controles en entidades públicas diciembre 2020 – Versión 5.

Tabla 31. Matriz Mapa Riesgos de Seguridad de la Información

	MATRIZ MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	Código: F-TIC-1400-238,37-047 Versión: 0.0 Fecha aprobación: Noviembre-24-2022 Página: 1 de 1

Proceso	Referencia	Activo de información	Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raíz)	Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de Riesgo inherente	No Control	Control Anexo A	Descripción del control	Afectación		Atributos								Probabilidad residual	Impacto residual	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento	Plan de Acción	Responsable	Fecha de Implementación	Seguimiento	Estado
																	Probabilidad	Impacto	Tipo	%	Implementación	%	Calificación del Control	Documentación	Frecuencia	Evidencia												

ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la siguiente tabla:

Tabla 32. Acciones de respuesta a riesgos materializados

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	**Líder de Proceso**	•Informar al Proceso de Planeación y Direccionamiento Estratégico sobre el hecho encontrado. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. • Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Actualizar el mapa de riesgos.
	Oficina de Control Interno de Gestión	• Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos
Riesgos de Gestión y Seguridad de la Información (Zona Extrema, Alta y Moderada)	**Líder de Proceso**	• Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el Plan de mejoramiento. • Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. • Analizar y actualizar el mapa de riesgos. • Informar al Proceso de Planeación y Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.
		• Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.
Riesgos de Gestión y Seguridad de la Información (Zona Extrema, Alta y Moderada)	**Oficina de Control Interno de Gestión**	•Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

Riesgos de Proceso y Seguridad de la Información (Zona Baja)		•Informar al líder del proceso sobre el hecho • Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

Fuente: Política de Operación para la Administración del Riesgo en Función Pública

COMUNICACIÓN Y SOCIALIZACIÓN DE LA POLITICA DE ADMINISTRACIÓN DE RIESGOS

La Política de Administración de Riesgos y los Mapas de Riesgos, se comunicarán y socializarán a todos los servidores públicos de la Alcaldía del Municipio de Bucaramanga, a través de los diferentes medios de comunicación con que cuenta la Entidad.

La Administración del Riesgo se considera un tema de gran importancia para la Administración Municipal. Por ello, se definirán jornadas de socialización internas y externas que garanticen la competencia necesaria de los servidores para atender el tema de una manera adecuada.

En tal sentido, se requiere que los líderes de proceso fortalezcan el manejo conceptual y operativo en todo lo relacionado con el riesgo.

MONITOREO Y SEGUIMIENTO INTEGRAL - ROLES LÍNEAS DE DEFENSA

12.1 INSTITUCIONALIDAD

El Modelo Integrado de Planeación y Gestión – MIPG establece que la gestión del riesgo es una responsabilidad directa del equipo directivo, la cual debe ejercerse desde el componente de direccionamiento estratégico y planificación institucional. En este contexto, es fundamental que se definan y emitan lineamientos claros para el tratamiento, manejo y seguimiento de los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos de la entidad.

Para asegurar una operación articulada y efectiva de esta política, el MIPG contempla la creación y funcionamiento de dos instancias clave en todas las entidades públicas: el Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Decreto 0175 del 27 de octubre de 2022; y el Comité Institucional de Coordinación de Control Interno, reglamentado mediante el artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017. En este marco general, ambos comités cumplen un rol determinante en la adecuada gestión del riesgo, operando de la siguiente manera:

Figura 14. Operatividad Institucional para la Gestión del Riesgo

12.2 MONITOREO Y SEGUIMIENTO

Los lideres de proceso en conjunto con su equipo de trabajo deben registrar los avances en el mapa de riesgos y analizar el estado de sus procesos frente a los controles establecidos.

En esta fase se debe:

a) Garantizar que los controles son eficaces y eficientes.
b) Obtener información adicional que permita mejorar la valoración del riesgo.
c) Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
d) Detectar cambios en el contexto interno y externo.
e) Identificar riesgos emergentes.

Nota: El monitoreo y revisión permite determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los factores de riesgo, así como su identificación, análisis y valoración.

12.2.1 Monitoreo y revisión:

✓ Primera Línea de Defensa: Los **líderes** de proceso con su equipo deben monitorear y revisar periódicamente los mapas de riesgos, con el fin de asegurar que las acciones establecidas se están llevando a cabo y evaluar la eficacia en su implementación, para evidenciar aquellas situaciones que pueden influir en la aplicación de acciones preventivas.

✓ Segunda Línea de Defensa: Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de procesos (dos veces al año).

12.2.2 Seguimiento:

✓ Tercera Línea de Defensa: La Oficina de Control Interno de Gestión, es la encargada de adelantar el seguimiento a los riesgos consolidados en el Mapa de Riesgos (dos veces al año). Para tal efecto, los responsables de cada proceso deben aportar los soportes y registros que validen el avance en la ejecución de las acciones propuestas.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.
- El seguimiento adelantado por la Oficina de Control Interno de Gestión se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.