2025

POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

ALCALDÍA DE
BUCARAMANGA

MUNICIPIO DE BUCARAMANGA

Versión 10.0

POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

MUNICIPIO DE BUCARAMANGA

Secretaría de Planeación	Planeación y Direccionamiento Estratégico
	Mejoramiento Continuo

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE AJUSTES**	**RESPONSABLE**
0.0	29 de marzo de 2017	Original	Profesional Especializado
1.0	Mayo de 2017	Se incluyeron los riesgos transversales y códigos de formatos y guía.	Profesional Especializado
2.0	18 de enero de 2019	Actualización documental, teniendo en cuenta la Guía para la administración del riesgo del DAFP 2018	Profesional Especializado
3.0	28 de abril de 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 de julio de 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 de noviembre de 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 de noviembre de 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 de septiembre de 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	25 de junio de 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
9.0	11 de septiembre de 2025	Actualización capítulo VI. Lineamientos de la Política de Administración de Riesgos, numeral 6.1 Niveles de Responsabilidad – Esquema de Líneas de Defensa. Aprobado en Comité Institucional de Coordinación de Control Interno según acta No. 13 del 9 de septiembre de 2025 y en Comité Institucional de Gestión y Desempeño de la Administración Central de Bucaramanga según acta No. 4 del 11 de septiembre de 2025.	Profesional Especializado
10.0	23 de diciembre de 2025	Actualización del contenido de acuerdo con la Guía de Gestión Integral del Riesgo y Diseño de Controles – Versión 7 (DAFP, 2025). Aprobado en Comité Institucional de Coordinación de Control Interno según acta No. 17 del 2 de diciembre de 2025.	Profesional Especializado

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

La Alcaldía de Bucaramanga, comprometida con el fortalecimiento de una gestión pública íntegra, transparente y orientada al valor público, reconoce la importancia de anticiparse a situaciones que puedan afectar el desempeño institucional y la confianza de la ciudadanía. En este sentido, la Gestión Integral del Riesgo constituye un pilar fundamental para mejorar la toma de decisiones, proteger los recursos públicos y garantizar la calidad y continuidad de los servicios ofrecidos a los ciudadanos.

Esta versión actualiza la Política conforme a los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (DAFP, 2025) e integra los requisitos del Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno – MECI, el Programa de Transparencia e Integridad Pública (PTEP), así como los marcos vigentes para la administración de riesgos de gestión, fiscales, de seguridad de la información y del Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP.

La Política para la Gestión Integral de Riesgos refleja el compromiso del equipo directivo con una administración basada en la prevención, la responsabilidad y el buen gobierno, articulando este enfoque con la planificación estratégica, el desempeño institucional, los procesos institucionales y la cultura organizacional. Así mismo, incorpora el esquema de líneas de defensa y se integra con los instrumentos de dirección, seguimiento y control de la Administración Municipal.

Su implementación requiere la participación activa de todos los servidores públicos, contratistas y colaboradores, quienes cumplen un rol esencial en la identificación, análisis, reporte, tratamiento, monitoreo y evaluación integral a los riesgos. De esta manera, la Alcaldía de Bucaramanga avanza hacia una administración resiliente y transparente, fortaleciendo el Sistema de Control Interno, la mejora continua y la prestación de un servicio efectivo a la ciudadanía.

1. CONDICIONES GENERALES DE LA POLÍTICA DE GESTIÓN INTEGRAL DE RIESGOS

La Alcaldía de Bucaramanga establece la gestión integral de riesgos como un proceso estratégico y obligatorio, alineado con los estándares internacionales ISO 31000:2018 y el Modelo Integrado de Planeación y Gestión (MIPG), con el fin de garantizar la eficiencia en la gestión pública y el logro de los objetivos institucionales. Establece directrices claras para integrar la gestión del riesgo en todas las actividades de la Alcaldía, garantizando liderazgo y compromiso de la Alta Dirección, asignación de recursos adecuados, definición de responsabilidades y mecanismos de seguimiento y monitoreo en todos los niveles organizacionales.

1.1. OBJETIVO DE LA POLÍTICA

Establecer los lineamientos institucionales que orientan la identificación, análisis, valoración, tratamiento, monitoreo y comunicación de los riesgos que puedan afectar el cumplimiento de los objetivos de la Alcaldía de Bucaramanga, fortaleciendo la gobernanza institucional, la toma de decisiones informada y la generación de valor público, en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG y los lineamientos nacionales en materia de gestión integral del riesgo; asegurando la integridad, transparencia y eficiencia en la administración de los recursos, y promoviendo una cultura organizacional orientada a la prevención y gestión proactiva de riesgos, que contribuya al cumplimiento de la misión institucional, la mejora continua y la confianza ciudadana en el municipio de Bucaramanga.

1.1.1. Objetivos Específicos

- Orientar la identificación, análisis y valoración de los riesgos institucionales, incluyendo los de gestión, fiscales, seguridad de la información e integridad pública.
- Definir criterios para el tratamiento, seguimiento y monitoreo de los riesgos, asegurando decisiones informadas y coherentes con los objetivos institucionales.
- Fortalecer la gobernanza y el sistema de control interno, articulando la gestión del riesgo con las líneas de defensa, MIPG y MECI.
- Promover una cultura organizacional preventiva y proactiva, involucrando a servidores públicos y contratistas en la identificación y gestión del riesgo.
- Asegurar la integridad, transparencia y eficiencia en la administración de los recursos públicos, mediante controles adecuados y mecanismos de supervisión.
- Contribuir al mejoramiento continuo y a la generación de valor público, integrando la gestión del riesgo con la planificación y la toma de decisiones basada en evidencia.

1.2. ALCANCE

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

1.3. CONTEXTO DE LA 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 SIIF
	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)
CONTEXTO INTERNO	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
	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

CONTEXTO INTERNO DEL PROCESO	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
	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
	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 ejecución
	Comunicación entre los	Mecanismos de articulación entre los procesos (reuniones, canales, mecanismos de seguimiento).
	Activos de Seguridad Digital del proceso	Procedimientos y estructura de matrices inventario de activos de información, Riesgos de Seguridad de la información

1.4. NIVELES DE RESPONSABILIDAD – ESQUEMA DE LÍNEAS DE DEFENSA

En coherencia con el Esquema de Líneas definido por el Modelo Integrado de Planeación y Gestión – MIPG, la Alcaldía de Bucaramanga adopta los siguientes niveles de responsabilidad para el seguimiento, control y mejora de los riesgos, distribuidas en varias áreas, no siendo una tarea exclusiva de la Oficina de Control Interno de Gestión, ya que dicha oficina hace parte del Sistema de Control Interno de forma integral, de allí que deban ser coordinadas para asegurar que los controles operen en la entidad:

Línea estratégica de defensa: Está conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

Primera línea de defensa: Esta línea está conformada por todos los servidores públicos de la entidad, quienes en el ejercicio de sus funciones son responsables de aplicar los controles internos en el desarrollo de las actividades diarias. Cuando se trata de jefes, líderes o responsables de proceso, estos ejercen controles de gerencia operativa, en tanto asumen la responsabilidad de orientar y supervisar la correcta gestión de los riesgos en sus procesos.

Segunda línea de defensa: Esta línea de defensa está conformada por los servidores públicos que desempeñan cargos del nivel directivo o asesor, quienes ejercen funciones de supervisión sobre asuntos transversales de la entidad y rinden cuentas ante la Alta Dirección.

Dentro de esta línea se incluyen, según la estructura institucional, la Secretaría de Planeación, Secretarías de despacho, Jefes de oficina, Proceso de Mejora Continua de la Secretaría Administrativa, Área de contratación de la Secretaría Jurídica, Secretaría de Hacienda y Área TIC. El ejercicio de esta línea de defensa permite a la entidad realizar un seguimiento y autoevaluación permanente de la gestión, orientando y generando alertas tanto a los servidores de la primera línea de defensa como a la Alta Dirección.

Tercera línea de defensa: Esta línea de defensa está conformada por la Oficina de Control Interno de Gestión.

Tabla 3. *Responsabilidades Líneas de Defensa frente al riesgo*

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Estratégica	Alta Dirección - Alcalde Municipal, Comité Institucional de Coordinación de Control Interno	• Emitir, revisar, validar y supervisar el cumplimiento de políticas en materia de control interno, seguimientos a la gestión y auditoría interna para toda la entidad. • Definir, aprobar y evaluar la Política para la Gestión Integral de Riesgos, su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo y riesgos emergentes. • Aplicar el monitoreo correspondiente a los riesgos críticos, utilizando la información suministrada por las instancias de segunda línea. • Analizar los resultados del monitoreo para identificar incumplimientos, retrasos o posibles actuaciones irregulares. • Tomar acciones oportunas de intervención frente a las situaciones detectadas. • Prevenir consecuencias para la entidad derivadas de la materialización de riesgos. • Analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP
Primera Línea	Líderes o responsables de proceso, servidores y colaboradores	• Identificar los riesgos y establecer controles, así como su monitoreo, acorde con el diseño de dichos controles, evitando la materialización de los riesgos y proponer mejoras a la gestión del riesgo en su proceso. • Mantener efectivos los controles internos, por consiguiente, identificar, evaluar, controlar y mitigar los riesgos de los programas, proyectos, planes y procesos a su cargo. • Informar a la 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. • Ejecutar el monitoreo de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.
Segunda Línea	Secretaria de Planeación, Secretarías de despacho, Jefes de oficina, Proceso de mejora continua de la Secretaría Administrativa, Área TIC, Área de contratación de la Secretaría Jurídica,	• Asegurar que los controles y procesos de gestión del riesgo (sistemas de gestión de calidad, contratación y financiera) de la 1ª línea de defensa sean apropiados y funcionen correctamente. • Supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos. • Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: Riesgos y controles; Indicadores de gestión y Procesos y procedimientos. • Asesorar y acompañar a los líderes de procesos y equipos en la identificación, análisis y valoración de riesgos de contratación, riesgos para la defensa jurídica y riesgos emergentes.

	Secretaría de Hacienda	**Secretaría de Planeación:** • Asesorar y acompañar a los líderes de procesos y equipos en la identificación, análisis y valoración de riesgos institucionales. • Consolidar los Mapas de Riesgos (corrupción, gestión y fiscales) y presentarlos para análisis, aprobación y seguimiento ante el Comité Institucional de Coordinación de Control Interno y Comité de Gestión y Desempeño Institucional. • Revisar y consolidar los respectivos ajustes de acuerdo con las solicitudes de los líderes de proceso, para su inclusión y actualización de los mapas de riesgos • 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 conforme a la periodicidad establecida. • En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento que se desarrolla en el numeral 9.5.2
		Área 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 • Presentar al Comité Institucional de Gestión y Desempeño, el monitoreo a la eficacia de los controles de los riesgos de seguridad de la información, acorde con la información suministrada por los responsables de procesos
Tercera Línea	Oficina de Control Interno de Gestión	• 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 de riesgos. • Realizar seguimiento al Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.

Fuente: Creación Secretaría de Planeación, 2025

2. DEFINICIONES Y/O ABREVIATURAS

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 Integral del Riesgo:** Conjunto de actividades para identificar, analizar, valorar y tratar los riesgos que afectan la operación, la integridad pública, la seguridad de la información y la gestión fiscal.
- **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.

- **KRI – Indicadores Clave de Riesgo:** Variables que alertan sobre cambios o comportamientos inusuales que pueden anticipar materializaciones.
- **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 emergente:** Es un riesgo nuevo o en evolución, con información limitada sobre su probabilidad e impacto, que puede afectar significativamente los objetivos

institucionales. Se caracteriza por su novedad, incertidumbre y potencial impacto, generalmente asociado a cambios sociales, tecnológicos, normativos, ambientales o políticos (ej.: ciberseguridad, cambios normativos, crisis sanitarias).

- **Riesgo Inherente**: Nivel de riesgo antes de implementar controles
- **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.

3. ARTICULACIÓN DE LA GESTIÓN INTEGRAL DE RIESGOS CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG

La Gestión Integral de Riesgos en la Alcaldía de Bucaramanga se articula de manera transversal con las dimensiones, políticas e instancias del Modelo Integrado de Planeación y Gestión – MIPG, consolidándose como un componente estratégico para la toma de decisiones, la planeación, el control y la mejora del desempeño institucional. Esta integración asegura que la administración del riesgo esté incorporada en todas las fases del ciclo de gestión pública y contribuya al valor público.

A continuación, se describe su alineación con cada dimensión del Modelo:

- **Planeación Institucional y Estratégica:** La gestión del riesgo es un insumo obligatorio para la formulación y actualización del Plan de Desarrollo Municipal, el Plan de Acción Institucional, los planes estratégicos, la definición de metas, la programación presupuestal y la gestión del desempeño. Los riesgos estratégicos orientan decisiones sobre prioridades, inversiones, asignación de recursos y ajustes en la planificación. Los riesgos de integridad pública (SIGRIP) y fiscales se integran como elementos críticos de diseño de controles y sostenibilidad financiera.
- **Gestión para el Servicio al Ciudadano:** El análisis de riesgos se incorpora en la operación de trámites, servicios y canales de atención (presenciales, digitales y telefónicos), para garantizar continuidad, calidad y seguridad. La articulación incluye riesgos operativos, de seguridad digital, disponibilidad tecnológica y protección al usuario.
- **Gestión del Talento Humano:** La gestión del riesgo se articula con la selección, inducción, capacitación y evaluación de los servidores, incorporando competencias en integridad, autocontrol, seguridad de la información y reporte de riesgos. Se fortalece así una cultura institucional preventiva y orientada a la integridad.
- **Direccionamiento Estratégico y Desempeño Institucional:** Los riesgos son insumo clave para orientar las decisiones de la Alta Dirección, los comités institucionales y el seguimiento a metas e indicadores. La gestión del riesgo permite identificar desviaciones, tomar decisiones oportunas y ajustar acciones del ciclo de desempeño.
- **Evaluación de Resultados:** El seguimiento, monitoreo y evaluación de los riesgos se articula con el seguimiento al Plan de Acción, la rendición de cuentas, los informes a entes de control y la evaluación independiente de la Oficina de Control Interno. Esto permite adoptar medidas correctivas y generar aprendizajes institucionales.
- **Información y Comunicación:** La gestión del riesgo depende de información confiable, oportuna y protegida. Por ello se articula con los sistemas de información institucionales, el Modelo de Seguridad y Privacidad de la Información (MSPI), la gestión documental, la protección de datos personales y la comunicación interna y externa.
- **Control Interno:** La gestión del riesgo es eje del MECI y opera bajo el enfoque de líneas de defensa:

Primera línea: líderes de proceso y equipos operativos, responsables de identificar, evaluar y tratar riesgos.

Segunda línea: áreas transversales como Secretaría de Planeación, Secretarías de despacho, Jefes de oficina, Proceso de mejora continua de la Secretaría Administrativa, Área TIC, Área de contratación de la Secretaría Jurídica, Secretaría de Hacienda, que acompañan y monitorean la gestión del riesgo.

Tercera línea: evaluación independiente realizada por la Oficina de Control Interno de Gestión.

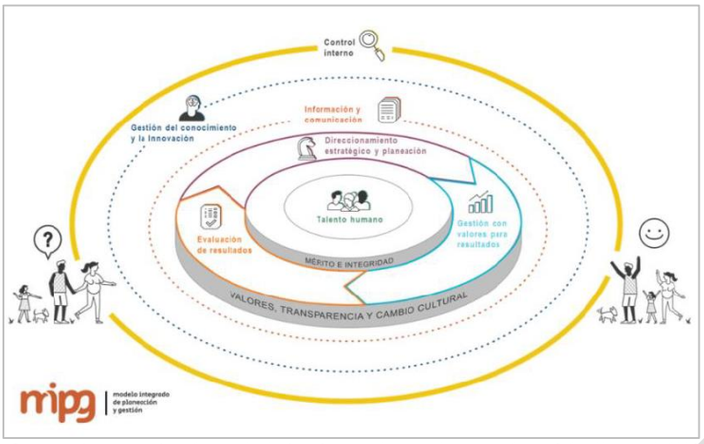
Por otra parte, en cumplimiento de la Guía de Gestión Integral del Riesgo y Diseño de Controles Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (DAFP, 2025), las siguientes políticas mantienen una articulación prioritaria con la gestión del riesgo por su incidencia directa en la prestación del servicio y el cumplimiento misional:

- **Integridad:** identificación y control de riesgos de corrupción, fraude, conflicto de interés, soborno y afectaciones a la ética pública, mediante la implementación del SIGRIP.
- **Talento Humano:** desarrollo de competencias en autocontrol, reporte de riesgos, seguridad de la información e integridad, fortaleciendo la cultura preventiva.
- **Servicio al Ciudadano:** gestión de riesgos que afecten la calidad, continuidad, oportunidad y accesibilidad de los servicios y trámites.
- **Gobierno Digital y Seguridad de la Información:** identificación y tratamiento de riesgos de ciberseguridad, protección de datos, continuidad tecnológica, vulnerabilidades y fallas en sistemas y plataformas.
- **Gestión de Información y Datos:** aseguramiento de la calidad, disponibilidad, integridad, trazabilidad y uso adecuado de los datos institucionales.
- **Gestión Documental:** prevención de riesgos de pérdida, alteración, deterioro o indisponibilidad de documentos oficiales y de la memoria institucional.
- **Participación Ciudadana:** gestión de riesgos asociados a la interacción con grupos de interés, procesos de consulta y control social.
- **Defensa Jurídica:** identificación y tratamiento preventivo de riesgos legales y contingencias que puedan generar impacto patrimonial.
- **Control Interno:** fortalecimiento de controles preventivos, detectivos y correctivos con base en el esquema de líneas de defensa.
- **Planeación Institucional:** incorporación obligatoria del análisis del riesgo en la formulación del Plan de Desarrollo, Plan de Acción, proyectos y metas estratégicas.

Adicionalmente, la gestión de riesgos se articula de manera operativa con las políticas de contratación, presupuesto, gestión del conocimiento, racionalización de trámites, seguimiento y evaluación.

De esta forma, la Alcaldía de Bucaramanga asegura que la Gestión Integral de Riesgos sea un componente estratégico, coherente y articulado del MIPG, fortaleciendo la gobernanza, la integridad, la eficiencia institucional y la confianza ciudadana.

***Figura 1**. Esquema general del modelo integrado de planeación y gestión (MIPG)*



Fuente: Departamento Administrativo de la Función Pública, MIPG, 2017.

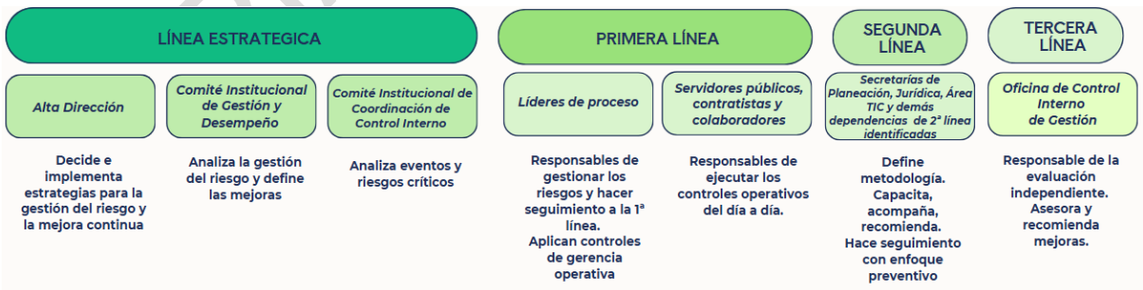
3.1. INSTITUCIONALIDAD PARA LA GESTIÓN INTEGRAL DE RIESGOS

La institucionalidad para la Gestión Integral del Riesgo en la Alcaldía de Bucaramanga se estructura a partir del Modelo Integrado de Planeación y Gestión – MIPG, del Modelo Estándar de Control Interno – MECI, del Manual MIPG V3.0 adoptado por la Administración Municipal y de los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (DAFP, 2025). Esta institucionalidad garantiza que la gestión del riesgo sea una función transversal e integrada a los procesos, políticas, instrumentos de dirección y toma de decisiones de la entidad.

Desde esta perspectiva, la gestión del riesgo involucra a toda la organización y se articula con el esquema de líneas de defensa**,** tal como lo orienta la Guía DAFP v7, donde los comités MIPG y de control interno cumplen roles esenciales para asegurar decisiones estratégicas y la eficacia del Sistema de Control Interno.

A continuación, se define cómo opera esta institucionalidad en el contexto específico de la Alcaldía de Bucaramanga:

***Figura 2.** Institucionalidad del MIPG desde la perspectiva de Gestión de Riesgo*



Fuente: Secretaría de Planeación

Articulación con instancias municipales adicionales. La institucionalidad de la Alcaldía incluye la interacción con los siguientes órganos establecidos en el Manual MIPG V3.0:

- Comité Municipal de Gestión y Desempeño (Decreto 0176 de 2022)
- Comité Municipal de Auditoría, que integra entidades descentralizadas y apoya la supervisión del control interno.

Estos comités fortalecen la coordinación interinstitucional y contribuyen a la consistencia en la gestión del riesgo entre las entidades del municipio.
De esta forma, la Alcaldía de Bucaramanga asegura que la Gestión Integral de Riesgos sea un componente estratégico, coherente y articulado del MIPG, fortaleciendo la gobernanza, la integridad, la eficiencia institucional y la confianza ciudadana.

3.1.1. Beneficios de la Gestión Integral del Riesgo. La Gestión Integral del Riesgo aporta valor a la Alcaldía de Bucaramanga al fortalecer la capacidad institucional para anticipar y enfrentar situaciones que puedan afectar el logro de los objetivos misionales. Entre sus principales beneficios se destacan:

- **Mayor efectividad en el cumplimiento de objetivos**, al orientar decisiones y controles hacia la prevención y la corrección oportuna de desviaciones.
- **Continuidad y estabilidad en la operación**, al reducir la probabilidad e impacto de eventos que puedan interrumpir la prestación de servicios o afectar procesos críticos.
- **Fortalecimiento de una cultura preventiva e íntegra**, promoviendo el compromiso de servidores y contratistas con el autocontrol, la transparencia y el uso responsable de los recursos públicos.

Estos beneficios consolidan la Gestión Integral del Riesgo como un componente esencial del buen gobierno y del fortalecimiento del Sistema de Control Interno en la Administración Municipal.

3.1.2. Aspectos clave antes de aplicar la metodología. La Alcaldía de Bucaramanga establece la gestión integral de riesgos como un proceso estratégico que integra cultura organizacional, capacidades, técnicas, estrategia y desempeño, para crear y proteger valor público.

Se promueve:

- Una **cultura de riesgos** liderada desde la Alcaldía, fortalecida en todos los niveles mediante comportamientos y decisiones coherentes con los objetivos institucionales.
- El **desarrollo de capacidades** para identificar, anticipar y gestionar riesgos, asegurando la mejora continua y la adaptación al cambio.
- La **aplicación de técnicas** dinámicas y conocidas por todos los funcionarios, facilitando la toma de decisiones y el uso eficiente de los recursos públicos.
- La **integración con la estrategia y objetivos**, garantizando que la gestión del riesgo contribuya a la misión, visión y satisfacción de las necesidades de la ciudadanía.

La **evaluación de niveles de madurez**, siguiendo el modelo COSO-ERM, para identificar prioridades de mejora y fortalecer la gestión integral de riesgos en toda la Alcaldía.

4. NORMOGRAMA

La presente política se sustenta en la normativa nacional e internacional vigente que orienta la gestión integral de riesgos en entidades públicas, asegurando transparencia, control, eficiencia, integridad y seguridad de la información. Entre los principales referentes normativos y lineamientos se encuentran:

Norma	Año	Objeto / Pertinencia para la Política
Constitución Política de Colombia	1991	Establece los principios generales de la función pública, control interno y buen gobierno.
Ley 87	1993	Regula el ejercicio del control interno en entidades públicas. En el art. 2 literal f) establece como objetivo prevenir riesgos y corregir desviaciones que afecten los objetivos institucionales.
Ley 489	1998	Establece la organización y funcionamiento de la Administración Pública, marco general para la gestión institucional.
Ley 610	2000	Regula los procesos de responsabilidad fiscal, vinculados a la gestión de riesgos en el uso de los recursos públicos.
Decreto 4485	2009	Actualiza la NTCGP 1000:2009. En el numeral 4.1 literal g) exige establecer controles sobre riesgos que puedan afectar satisfacción del cliente y objetivos institucionales.
Decreto 1083	2015	Decreto Único Reglamentario del Sector de Función Pública. Título 23 reglamenta la implementación obligatoria de la NTCGP 1000:2009 en entidades públicas.
Resolución 193 – Contaduría General de la Nación	2016	Incorpora en el Régimen de Contabilidad Pública el procedimiento para la evaluación del control interno contable.
Decreto 648	2017	Modifica y adiciona el Decreto 1083 de 2015 en materia de gestión pública.
Decreto 1499	2017	Ajusta el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Guía para la Administración del Riesgo y el diseño de controles – versión 4, Función Pública	2018	Lineamientos sobre riesgos de gestión, corrupción y seguridad digital en entidades públicas.
Anexo 4 – Guía DAFP 2018	2018	Lineamientos para la gestión de riesgos de seguridad de la información en entidades públicas.
Política de Operación de Riesgos – Función Pública	2018	Directriz para la implementación operativa de la gestión de riesgos en entidades públicas.
Norma Internacional ISO 31000	2018	Establece lineamientos internacionales para la gestión integral de riesgos.
Norma Técnica Colombiana ISO 9001	2015 (adoptada)	Define requisitos para los sistemas de gestión de calidad. En el numeral 6.1 exige

		acciones para abordar riesgos y oportunidades.
Ley 2195	2022	Establece medidas de transparencia, prevención y lucha contra la corrupción, integrando la gestión de riesgos como herramienta de prevención.
Guía para la Administración del Riesgo y el diseño de controles – versión 6, Función Pública	2022	Actualización de lineamientos para la gestión de riesgos, controles y seguridad digital en entidades públicas.
Resolución 0139 – Municipio de Bucaramanga	2023	Adopta la Política Institucional de Seguridad y Privacidad de la Información, normativa interna aplicable.
Decreto 1122	2024	Reglamenta los Programas de Transparencia y Ética Pública (art. 73 Ley 1474 de 2011 y art. 31 Ley 2195 de 2022). Refuerza la gestión de riesgos de corrupción y transparencia.
Guía para la Gestión Integral del Riesgo en Entidades Públicas– Versión 7, DAFP	2025	Lineamientos actualizados para identificación, evaluación, tratamiento, monitoreo y reporte de riesgos en entidades públicas.

5. DESARROLLO Y/O DESCRIPCIÓN

5.1. METODOLOGÍA GENERAL PARA LA GESTIÓN INTEGRAL DEL RIESGO

La Alcaldía de Bucaramanga adoptará un esquema metodológico unificado para la identificación, análisis, valoración y tratamiento de los riesgos, tomando como referencia los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas– Versión 7 del DAFP.

Figura 3. *Metodología General para la Gestión del Riesgo*

Fuente: Función Pública 2025

5.1.1. Marco sobre Apetito del Riesgo. La Alcaldía de Bucaramanga define el apetito del riesgo como el nivel de riesgo que la entidad está dispuesta a aceptar en el cumplimiento de sus objetivos institucionales, teniendo en cuenta su misión, visión y los principios de legalidad, transparencia y protección del recurso público.

La determinación del apetito del riesgo se realiza mediante un enfoque cualitativo, basado en la valoración de probabilidad e impacto definida en la metodología institucional. Su definición corresponde a la Alta Dirección y se aprueba en el Comité Institucional de Coordinación de Control Interno.

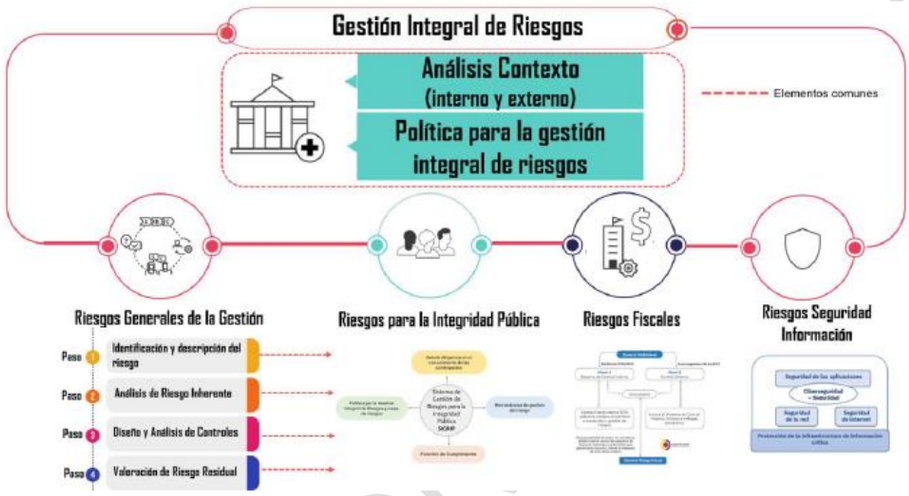
En la entidad se establece tolerancia cero frente a riesgos que impliquen conductas contrarias a la integridad pública, tales como: soborno, fraude, conflicto de intereses no gestionado, corrupción y riesgos de LA/FT/FP. Para los demás riesgos —de gestión, fiscales y de seguridad de la información— la entidad acepta niveles moderados de riesgo que permitan el cumplimiento de los objetivos sin comprometer la continuidad del servicio ni la confianza ciudadana.

La capacidad de riesgo de la entidad está determinada por sus obligaciones legales, sus competencias, su disponibilidad presupuestal y su responsabilidad en la protección del interés general. El apetito del riesgo será revisado de manera periódica y actualizado cuando se modifiquen los objetivos estratégicos, la estructura organizacional o las condiciones del entorno institucional.

5.1.2. Articulación de los Ámbitos para la Gestión Integral del Riesgo. La Alcaldía de Bucaramanga gestiona sus riesgos de manera integral, articulando los diferentes ámbitos que pueden afectar el cumplimiento de sus funciones: los riesgos de la gestión, los riesgos fiscales, los riesgos de seguridad de la información y los riesgos para la integridad pública.

Todos estos ámbitos comparten elementos comunes: el análisis del contexto institucional, la aplicación de la Política para la Gestión Integral de Riesgos y el uso de una metodología unificada para identificar, analizar y valorar los riesgos, así como para revisar los controles existentes y determinar el riesgo residual. Esta articulación permite que la entidad cuente con una visión completa y coherente de sus riesgos.

Figura 4. *Articulación ámbitos gestión del riesgo*



Fuente: Función Pública 2025

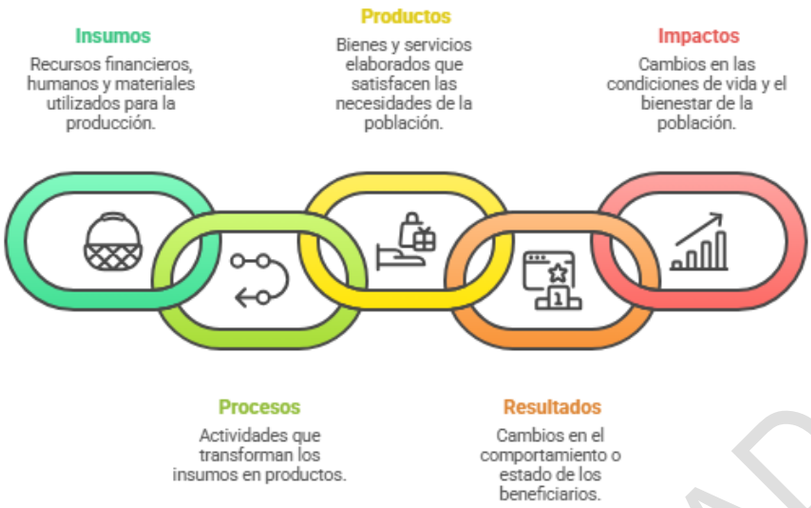
6. RIESGOS GENERALES DE LA GESTIÓN

Los riesgos generales de la gestión son aquellos asociados a la operación diaria de la Alcaldía y a los procesos que soportan su misión. Su identificación y tratamiento se realizan conforme a la metodología establecida en esta Política, considerando la naturaleza, objetivos y particularidades de cada proceso. Por ello, los mapas de riesgos pueden variar en número y complejidad entre dependencias, según sus actividades clave y la forma en que contribuyen a la prestación de servicios y al cumplimiento institucional.

6.1. PASO 1. IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

6.1.1. Identificación de riesgos clave: Cada dependencia identificará los eventos que puedan afectar el cumplimiento de los objetivos de su proceso, considerando las actividades clave, la cadena de valor y la interacción con otros procesos. Los riesgos deben describirse de manera clara y alineados con los objetivos institucionales.

***Figura 5**. Cadena de Valor*



Para identificar los puntos de riesgo clave, se deben analizar los productos, servicios y actividades del proceso que podrían verse afectados, así como el posible impacto en otros procesos dentro de la cadena de valor institucional.

***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.

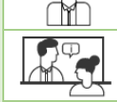
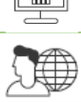
6.1.2. Identificación de áreas de impacto: Se determinará el tipo de impacto que podría generar cada riesgo, considerando dos categorías aplicables a la Alcaldía: afectación económica (o presupuestal) y afectación reputacional**.**

- **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.

- **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.

6.1.3. Identificación de factores de riesgo: Se identificarán las condiciones internas o externas que aumentan la probabilidad de ocurrencia del riesgo. La Alcaldía utilizará como referencia los factores definidos en esta Política, incluyendo aquellos relacionados con riesgos de integridad pública, y podrá ajustarlos según las particularidades de cada proceso.

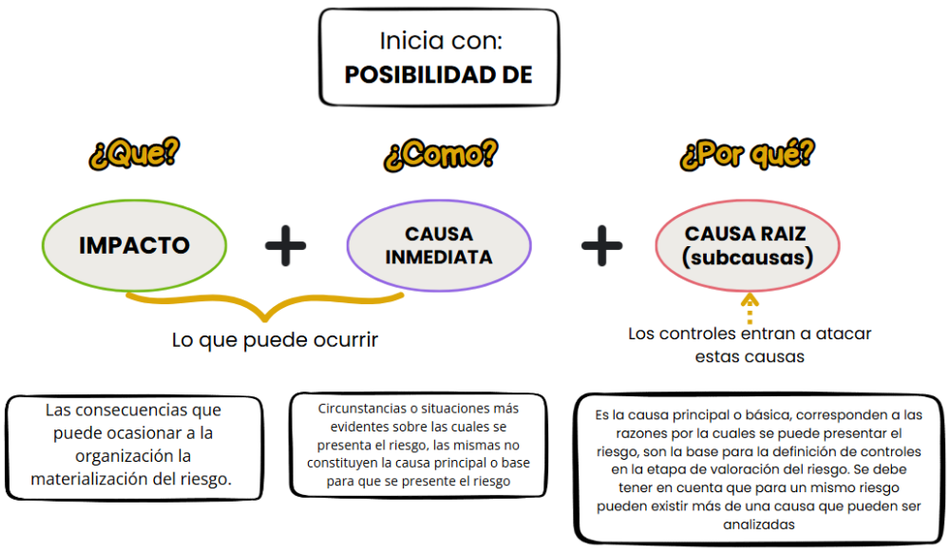
Tabla 5. *Factores de riesgo*

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

Fuente: Función Pública y Secretaría de Transparencia, 2025.

6.1.4. Descripción del Riesgo. Una vez identificado el punto de riesgo, el área de impacto y los factores de riesgo, se procede a redactar el riesgo. Para ello, se deben integrar tres elementos clave:

Figura 6. *Estructura propuesta para la redacción del riesgo*



Para asegurar una redacción adecuada, el riesgo debe ser específico, claro y orientado a describir qué podría pasar, por qué podría ocurrir y qué lo hace más probable.

En resumen, todo riesgo debe describirse respondiendo a:

- ¿Qué puede pasar? (evento)
- ¿Por qué puede pasar? (causas)
- ¿Qué consecuencias tendría? (impacto)
- ¿Qué condición incrementa su probabilidad? (factor de riesgo)

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. PASO 2. 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.

6.2.1. Determinar la probabilidad. Corresponde a la posibilidad de que el riesgo ocurra y se calcula con base en la frecuencia anual de la actividad que genera la exposición al riesgo. Este método reduce la subjetividad, pues se fundamenta en cuántas veces el proceso pasa por el punto de riesgo en un año, en lugar de basarse en eventos históricos que podrían no reflejar la realidad de la entidad.

La probabilidad se valorará siguiendo las escalas definidas por la entidad, tomando como referencia la periodicidad de actividades típicas de la gestión pública.

***Tabla 6**. Actividades relacionadas con la gestión en entidades públicas*

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

Nota: Para tecnología se considera que **1 hora de funcionamiento equivale a 1 vez**. Ejemplo: Si un aplicativo como el FURAG está disponible 24 horas durante 2 meses, su frecuencia se calcula así: **60 días × 24 horas = 1.440 horas (veces).**

***Tabla 7**. Criterios para definir el nivel de probabilidad*

Probabilidad	Frecuencia de la Actividad
Muy Baja 20%	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año
Baja 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta 80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Función Pública, 2025

6.2.2. Determinar el impacto. Corresponde a las consecuencias que puede generar la materialización de un riesgo en la entidad. Para su análisis, se establece dos tipos principales de impacto: **económico** y **reputacional**, agrupando en ellos aspectos antes evaluados por separado (como sanciones, indemnizaciones, afectación presupuestal o fallas en la prestación del servicio), con el fin de simplificar el análisis y reducir la subjetividad. Cuando un riesgo presente ambos tipos de impacto con niveles distintos, se deberá adoptar **el nivel más alto** para asegurar una valoración conservadora y coherente.

***Tabla 8.** Criterios para definir el nivel de impacto*

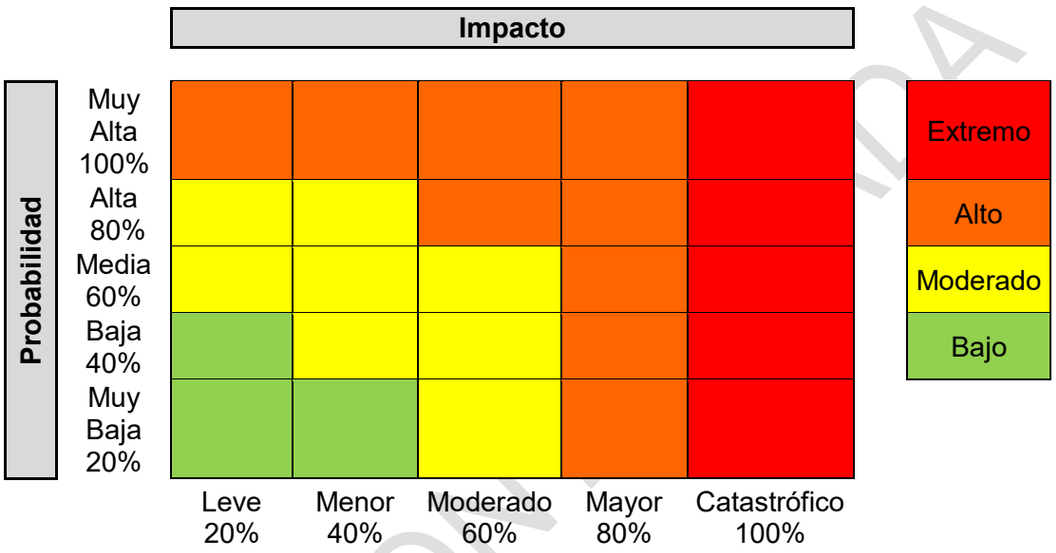
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor 40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.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

Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Función Pública, 2025

6.2.3. Análisis de Severidad. se determina combinando la probabilidad de ocurrencia y el impacto del riesgo. Esta valoración se representa en una matriz de calor con cuatro niveles de severidad**,** lo que permite establecer de manera clara qué tan crítico es un riesgo antes de considerar los controles existentes. A partir de esta combinación se obtiene la severidad del riesgo y su prioridad para la gestión institucional.

Figura 7. *Matriz de calor (niveles de severidad del riesgo)*



Fuente: Función Pública. 2025

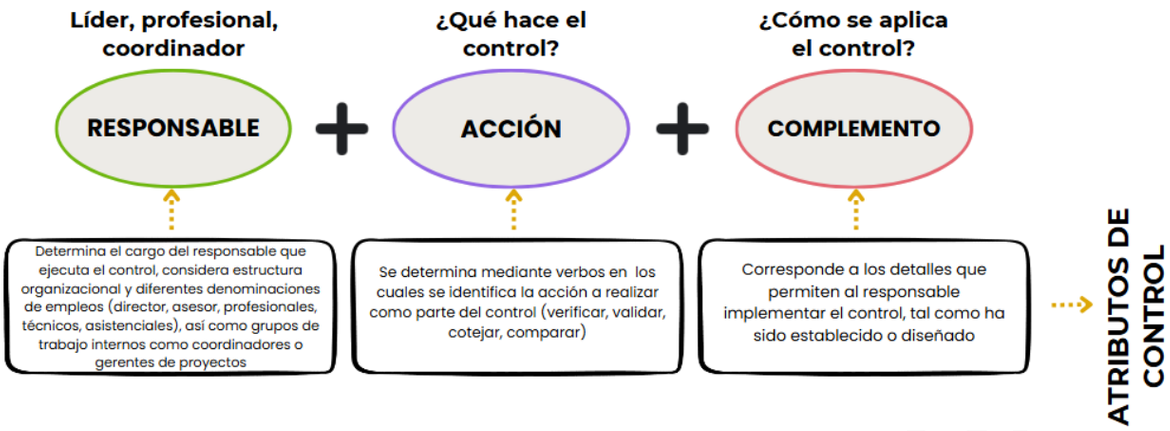
6.3. PASO 3. DISEÑO Y ANÁLISIS DE CONTROLES

El diseño de controles consiste en establecer acciones concretas que reduzcan la probabilidad o el impacto de los riesgos. Para ello, los controles deben:

- Diseñarse según el riesgo identificado, con base en entrevistas, documentación del proceso o análisis técnico.
- Incluir atributos claros como responsable, periodicidad, forma de ejecución y niveles de autoridad.
- Responder directamente a las causas raíz y factores de riesgo para asegurar su efectividad.

La descripción del control debe ser clara y contener los elementos que garanticen su correcta implementación por parte del responsable.

Figura 8. *Estructura para la redacción de controles*



6.3.1. 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.

Figura 9. *Tipologías de controles*

Fuente: Función Pública. 2025

6.3.2. 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 9. *Valoración de controles*

Características de Eficiencia		Descripción	Peso
Tipo	Preventivo	Accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado	25%

	Detectivo	Accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos	15%
	Correctivo	Se activan después de materializado el riesgo y suelen implicar costos, como pólizas de seguro, copias de seguridad o bancos de datos. Aunque requieren acciones previas, no son preventivos porque solo operan tras el evento, por lo que deben clasificarse siempre como controles correctivos.	10%
Implementación ***Nota:** En implementación no se tienen controles semiautomáticos.*	Automático	Ejecutados por un sistema o software previamente programado o diseñado.	25%
	Manual	Ejecutados por personas.	15%

Fuente: Función Pública, 2025

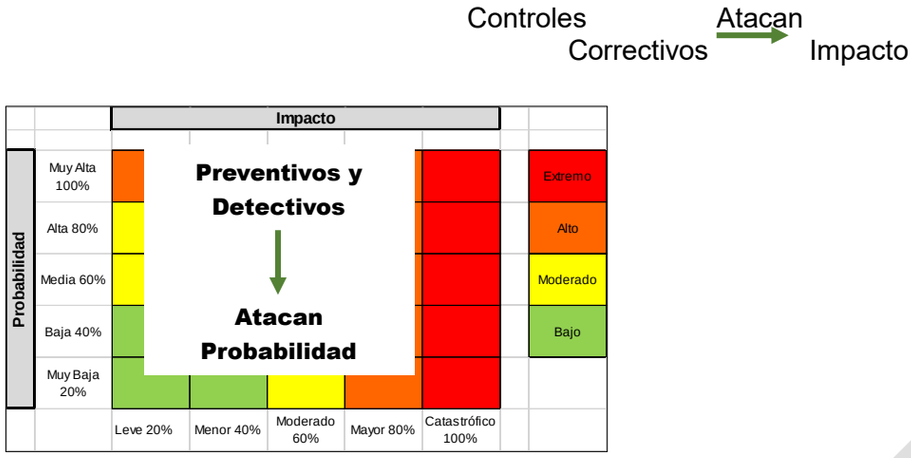
***Tabla 10.** Análisis atributos formalización del control*

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Función Pública, 2025.

6.3.3. Aplicación de Controles en la matriz de severidad. Los controles determinan el movimiento en la matriz de calor, afectando los ejes de probabilidad e impacto según su tipo.

Figura 10. *Movimiento en la matriz de calor acorde con el tipo de control*



Fuente: Función Pública. 2025

6.4. PASO 4. VALORACIÓN DE RIESGO RESIDUAL

Consiste en determinar el nivel de riesgo que permanece después de aplicar la efectividad de los controles al riesgo inherente. Los controles se aplican de forma acumulativa: cada control ajusta el valor resultante del anterior. El riesgo residual final refleja cuánto se reduce el riesgo tras considerar los controles preventivos, detectivos o correctivos existentes.

Ejemplo:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	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%**
	Valoración de Impacto				
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				**80%**

Una vez aplicada toda la metodología, se procede a elaborar los mapas de riesgos por proceso, utilizando matrices en Excel o, en entidades con mayor complejidad, herramientas especializadas que mantengan el mismo enfoque metodológico.

Consolidación del Mapa Integral de Riesgos: Finalizado el análisis por proceso, se construye el mapa integral de riesgos, que sintetiza los resultados en una matriz descriptiva y un esquema gráfico. Este consolidado debe integrar las tipologías de riesgo aplicables a cada proceso, considerando su complejidad, interacción con otros procesos, recursos,

productos, servicios y usuarios, garantizando así una visión completa e integral del riesgo institucional.

7. GESTIÓN PREVENTIVA DE RIESGOS FISCALES

La entidad incorpora la gestión preventiva de riesgos fiscales como parte integral de la Política, orientada a evitar daños al patrimonio público, entendidos como menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado (Ley 610 de 2000).

Para abordar la gestión preventiva del riesgo fiscal, es fundamental partir del concepto de gestión fiscal, el cual se compone de elementos que definen qué es, quién la realiza, qué actividades comprende y con qué propósito, tal como se presenta en la siguiente tabla:

***Tabla 11**. Concepto gestión fiscal - componentes*

¿Qué es?	¿Quién la realiza?	¿Qué comprende?	¿Para qué?
El conjunto de actividades económicas, jurídicas y tecnológicas	Los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos	La adecuada y correcta: • adquisición• planeación• conservación• administración• custodia• explotación• enajenación• consumo• adjudicación• gasto• inversión• disposición• recaudación• manejo• inversión de los bienes públicos y de sus rentas	En orden a cumplir los fines esenciales del Estado, con sujeción a los principios establecidos en el artículo 3 de la Ley 610 de 2000

Fuente: Función Pública 2025, con base en Ley 610/2000 art. 3.

La política reconoce el modelo de control fiscal definido por el Acto Legislativo 04 de 2019 y el Decreto 403 de 2020, el cual incorpora un enfoque preventivo y concomitante que complementa el control posterior y selectivo ejercido por los órganos de control. Este modelo se articula con el Sistema de Control Interno como una herramienta clave para fortalecer la vigilancia y la prevención del daño patrimonial, integrando ambos niveles de control y los conceptos que de esta articulación se derivan.

7.1. CONTROL FISCAL INTERNO Y PREVENCIÓN DEL RIESGO FISCAL

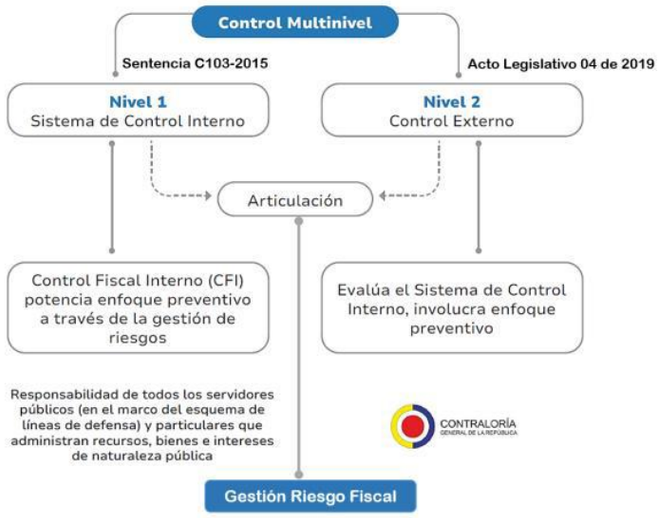
La gestión preventiva del riesgo fiscal se fundamenta en un modelo de control fiscal multinivel, que articula el Sistema de Control Interno como primer nivel de vigilancia con el control externo ejercido por los organismos de control, complementado por la participación del control social.

En este contexto, el **Control Fiscal Interno (CFI)** constituye el primer nivel de vigilancia para proteger el patrimonio público, prevenir riesgos fiscales y garantizar el uso adecuado de los recursos. Su ejercicio es responsabilidad de todos los servidores públicos y de los particulares que administran bienes o fondos del Estado, y su eficacia es evaluada por la Contraloría competente, siendo determinante para el fenecimiento de la cuenta.

La entidad identifica, analiza y gestiona los riesgos fiscales dentro de sus procesos como parte del Mapa Integral de Riesgos, con el propósito de anticipar situaciones que puedan

afectar los recursos públicos y adoptar medidas preventivas que contribuyan a su protección.

Figura 11. *Articulación modelo constitucional control fiscal y Sistema de Control Interno*



Fuente: Función Pública, 2022

7.2. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS FISCALES

La metodología propuesta orienta la gestión preventiva de los recursos, bienes e intereses patrimoniales públicos, con el fin de evitar daños fiscales y reducir la posibilidad de afectación al patrimonio por parte de los distintos gestores fiscales. Para apoyar este proceso, se dispone de un Catálogo Indicativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas, elaborado a partir del análisis de aproximadamente 130 fallos de responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República.

Este catálogo debe utilizarse como referencia para la identificación y valoración de riesgos fiscales, sin perjuicio de que cada entidad analice y determine puntos de riesgo adicionales conforme a su naturaleza, complejidad, recursos, sector y funcionamiento institucional.

El riesgo fiscal es el posible efecto dañoso sobre los recursos, bienes o intereses patrimoniales públicos, generado por un evento potencial, es decir, una acción u omisión incierta que podría causar dicho daño.

Este concepto incluye dos elementos clave:

- **Efecto dañoso:** la afectación que se produciría si el riesgo se materializa.
- **Evento potencial:** la acción u omisión que podría originar esa afectación.

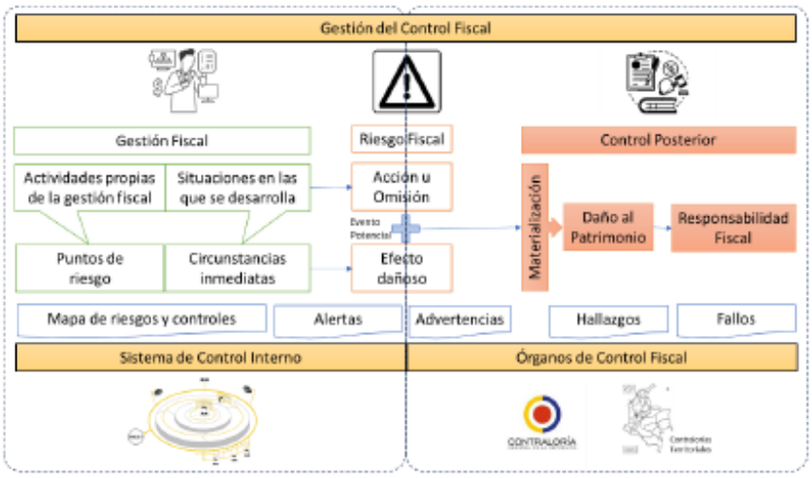
Lo anterior se puede resumir de la siguiente manera:

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

Es fundamental no confundir el riesgo fiscal con el daño patrimonial**:** el riesgo es la posibilidad de afectación, mientras que el daño patrimonial es la afectación real ya ocurrida.

La gestión del riesgo fiscal es responsabilidad de toda la entidad en el marco del Sistema de Control Interno, mientras que la determinación del daño patrimonial corresponde exclusivamente a los órganos de control fiscal.

Figura 12. *Gestión del Control Fiscal*



Fuente: Función Pública, 2025.

A continuación, se presentan los pasos para identificar, clasificar, valorar y controlar el **riesgo fiscal**. Aunque se presenta de manera independiente, su aplicación debe integrarse con la gestión de los riesgos estratégicos y operativos. Por ello, y siguiendo la metodología de cuatro pasos descrita en el Capítulo VI, se desarrollan a continuación los elementos específicos para la gestión del riesgo fiscal.

7.2.1. Paso 1. Identificación del Riesgo Fiscal. La identificación del riesgo fiscal inicia con el reconocimiento de los **puntos de riesgo**, es decir, actividades de la gestión fiscal donde existe potencial afectación al patrimonio público, especialmente aquellas asociadas a advertencias, alertas o hallazgos fiscales. Junto con estos puntos, deben identificarse las **circunstancias inmediatas**, que son situaciones evidentes en las que se manifiesta el riesgo, aunque no representan su causa raíz.

Este análisis debe desarrollarse con apoyo del personal directivo, asesor y servidores conocedores del proceso, y comprende cinco elementos básicos:

1. Identificación de puntos de riesgo y circunstancias inmediatas
2. Identificar el área de impacto
3. Identificar el posible efecto económico
4. Identificar la causa raíz
5. Descripción del riesgo fiscal.

La identificación de puntos de riesgo y las circunstancias inmediatas debe apoyarse en las siguientes preguntas orientadoras:

Tabla 12. *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	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo 1), son aplicables a la entidad?
Puntos de riesgo fiscal y	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

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

Fuente: Función Pública, 2025.

- **Identificación de áreas de impacto.** En el riesgo fiscal, el área de impacto siempre corresponde a una consecuencia económica sobre el patrimonio público en caso de materializarse el riesgo.

Para definir correctamente el impacto de un riesgo fiscal, es necesario tener claro el concepto de patrimonio público y sus tres expresiones según la Ley 610 de 2000, art. 6: bienes públicos, ii) recursos públicos y iii) intereses patrimoniales de naturaleza pública.

- **Identificación del efecto económico:** El efecto económico del riesgo fiscal corresponde al potencial detrimento, menoscabo, disminución, perjuicio, pérdida o

deterioro del patrimonio público derivado de un evento que pueda comprometer recursos, bienes o intereses de naturaleza pública. Aunque todos los riesgos fiscales generan un efecto económico, no todo efecto económico constituye un riesgo fiscal.

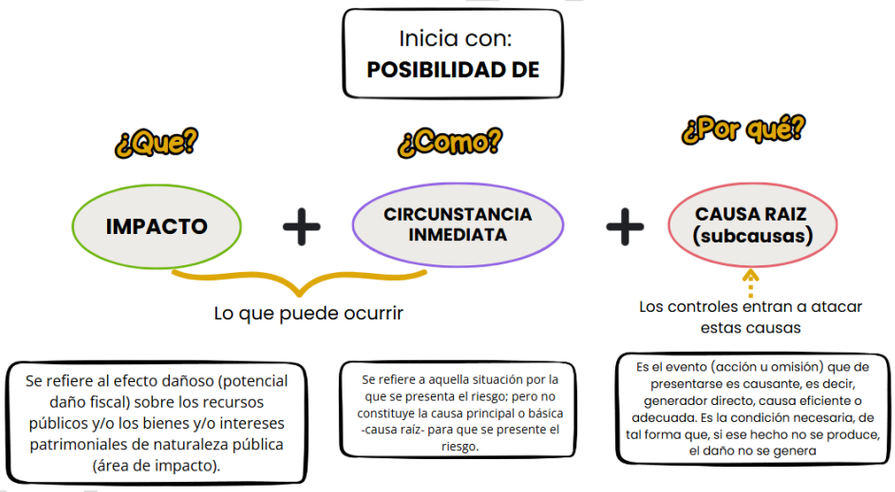
No se consideran riesgos fiscales, entre otros:

- ✓ Condenas y conciliaciones por daño antijurídico.
- ✓ Pérdidas originadas en fuerza mayor, caso fortuito o hechos de terceros sin calidad de gestor fiscal.
- ✓ Multas no asociadas a gestión fiscal.
- ✓ Actuaciones de cobro coactivo.
- ✓ Pérdidas normales por desgaste, uso ordinario o deterioro esperado de bienes.

- **Identificación de la causa raíz o potencial hecho generador.** La causa raíz es la acción u omisión que, de ocurrir, podría generar un daño al patrimonio público (menoscabo, pérdida o deterioro). Esta representa el evento potencial que origina el efecto dañoso y, por tanto, debe identificarse con objetividad y rigor, ya que los controles deben orientarse directamente a prevenirla. Es importante diferenciar claramente la causa raíz (lo que genera el riesgo) del daño fiscal (la consecuencia), evitando confundir el evento que provoca la afectación con la afectación misma.

- **Descripción del Riesgo Fiscal.** Consiste en redactar el riesgo fiscal integrando los elementos definidos previamente, apoyándose en los ejemplos del Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas (Anexo 1).

Figura 13. *Descripción riesgo fiscal*



Ejemplo 1:
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.

En la siguiente tabla se desarrollan los pasos antes explicados:

Paso	Identificación
Punto de Riesgo: (actividad de la gestión fiscal)	Administración de inmuebles en arrendamiento al servicio de la entidad

Circunstancia inmediata: (situación en la que se presenta el riesgo)	Pago de intereses moratorios en contrato de arrendamiento
Área de Impacto: (patrimonio público afectado)	Recursos públicos de la entidad
Efecto económico: (potencial daño al patrimonio)	Disminución de recursos disponibles equivalente al monto pagado por intereses moratorios
Causa raíz: (potencial acción u omisión)	Omisión del pago oportuno del canon de arrendamiento

Descripción del riesgo:

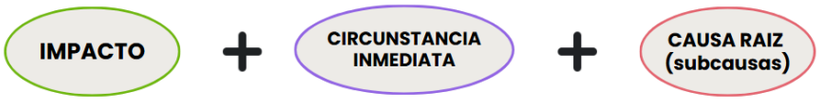
¿Qué?	¿Cómo?	¿Por qué?
Posible efecto dañoso sobre los recursos de la entidad	por la generación de intereses moratorios en contrato de arrendamiento	a causa de la omisión en el pago oportuno del canon pactado.

Conclusión: El hecho generador del daño no es el pago de la deuda ya que esta es una acción diligente que da cumplimiento a una obligación adquirida. La causa raíz corresponde a la omisión de pago oportuno y el riesgo fiscal al potencial daño representado en los intereses moratorios pagados. Ante dicha situación, se requiere la activación de controles correctivos para evitar que se materialice el daño patrimonial (Hallazgo fiscal), tales como el reembolso del monto correspondiente a los intereses moratorios y controles preventivos para que no se vuelva a presentar la omisión (causa raíz).

Ejemplo 2: *Proceso: Recaudo de impuestos*
Objetivo: Gestionar los ingresos tributarios establecidos a favor de la entidad, conforme al estatuto tributario y de procedimiento vigente.
Alcance: Inicia con la identificación de hechos gravables, sujetos pasivos y bases de liquidación de los impuestos establecidos a favor de la entidad y culmina con la expedición de paz y salvo a favor del contribuyente.

Paso	Identificación
Punto de Riesgo: (actividad de la gestión fiscal)	Gestión de cobro a contribuyentes en mora del pago de sus obligaciones tributarias.
Circunstancia inmediata: (situación en la que se presenta el riesgo)	Prescripción de los términos para la exigibilidad de las obligaciones tributarias.
Área de Impacto: (patrimonio público afectado)	Intereses patrimoniales de la entidad
Efecto económico: (potencial daño al patrimonio)	Menor recaudo de ingresos tributarios establecidos a favor de la entidad
Causa raíz: (potencial acción u omisión)	Errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Descripción del riesgo:



¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los intereses patrimoniales	por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora	a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Conclusión: El riesgo fiscal existe desde el momento en que, existiendo obligaciones en mora, los procedimientos de cobro no se ejecutan de manera oportuna y correcta, pues allí surge la potencial reducción del recaudo. En esta etapa, el sistema de control interno debe ser capaz de tomar los correctivos necesarios, pues una vez se materialice la prescripción, se configura el daño patrimonial (hallazgo fiscal) a partir del cual el órgano de control fiscal procede a establecer y exigir la responsabilidad del gestor fiscal.

A continuación, se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso:

Tabla 13. *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 implementación y operación de redes eléctricas seguras.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por negación del reconocimiento de siniestros en el contrato de seguro, a causa de la omisión en la actualización del inventario de bienes amparados.
Posibilidad de efecto dañoso sobre bienes públicos, por pérdida, extravío o hurto de bienes muebles de la entidad a causa de la inexistencia de procedimientos documentados para el ingreso y salida de bienes del almacén	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por menores ingresos percibidos sobre la explotación de marcas de propiedad comercial de la entidad a causa de errores u omisiones en el análisis técnico, jurídico y económico del mercado

Fuente: Función Pública, 2025

7.2.2. Paso 2: Valoración del riesgo fiscal: La valoración del riesgo fiscal permite establecer su nivel inherente, combinando la probabilidad de ocurrencia y el impacto económico que produciría su materialización.

- **Probabilidad:** corresponde al número de veces que la entidad realiza en un año la actividad asociada al punto de riesgo fiscal. A mayor frecuencia, mayor probabilidad inherente.
- **Impacto:** todo riesgo fiscal tiene impacto económico, pues implica un posible detrimento sobre recursos, bienes o intereses patrimoniales públicos. Su nivel se valora según la magnitud del daño potencial.
- **Riesgo inherente:** se determina combinando probabilidad e impacto, ubicándolo en una zona de severidad (baja, moderada, alta o extrema), utilizando las tablas de frecuencia, impacto y matriz de severidad definidas en la metodología institucional.

Manteniendo los criterios definidos para la evaluación definidos en el numeral 6.2.

7.2.3. Paso 3. Valoración de Controles: La valoración de controles permite determinar cómo las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Los controles pueden ser:

- **Preventivos:** actúan antes del evento para evitar la causa raíz.
- **Detectivos:** operan durante el evento para evitar que se materialice el daño.
- **Correctivos:** se activan después de ocurrido el evento para contener o reparar el daño potencial.

En la evaluación se analizan sus atributos (claridad, responsabilidad, segregación de funciones, formalización y eficiencia), siguiendo los lineamientos del control establecidos en el numeral 6.3 de la presente política. Esta valoración determina la capacidad real del control para mitigar el 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.*
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.*

Aplicando la tabla de valoración en los controles identificados, se tiene:

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	Tipo	Preventivo		
		Detectivo	X	**15%**

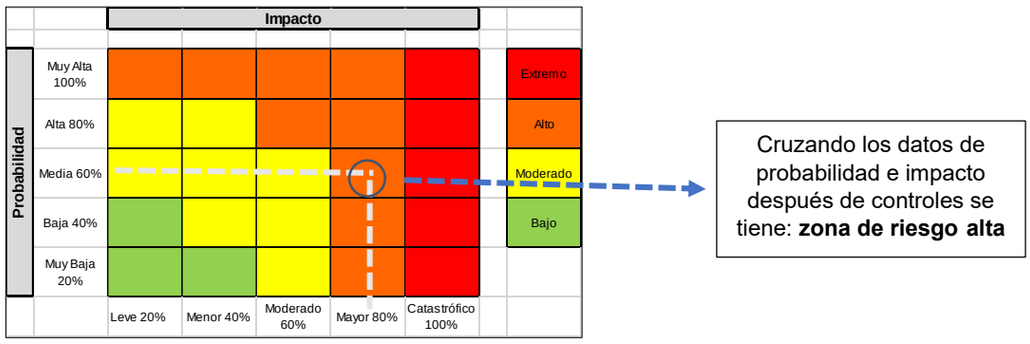
salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.		Correctivo		
	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%			

Nivel de riesgo (riesgo residual): La valoración del riesgo residual resulta de aplicar la efectividad de los controles al riesgo inherente. En la matriz de calor, cada tipo de control genera un movimiento específico sobre los ejes de **probabilidad** e **impacto**, según su naturaleza y valoración. Los controles se aplican de manera acumulativa: una vez se incorpora el efecto del primer control, el siguiente se calcula sobre el valor ajustado, y así sucesivamente. Esto permite establecer de forma objetiva cómo disminuye el nivel de riesgo hasta llegar al riesgo residual.

Con el fin de evidenciar el procedimiento, a continuación, se muestran los cálculos correspondientes a los tres controles establecidos en el ejemplo.

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%				

Los controles determinan el movimiento del riesgo en la matriz de calor. Según su tipo y valoración, modifican la probabilidad y el impacto del riesgo, permitiendo calcular el nivel residual resultante.



8. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

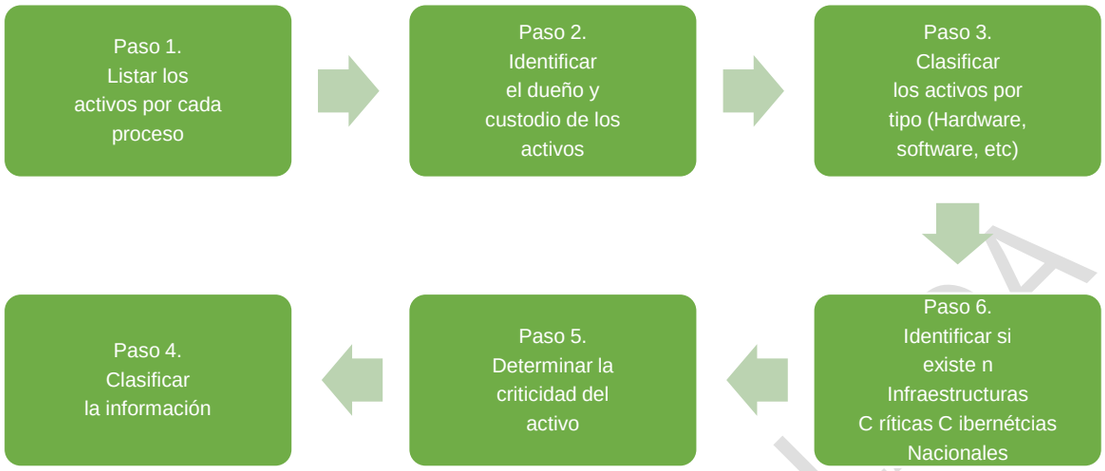
Dentro del componente de seguridad de la información, se identifican dos elementos fundamentales que, articulados adecuadamente, permiten alcanzar los objetivos establecidos en materia de seguridad de la información. El primer elemento, como insumo inicial, es el *Inventario de Activos de Información*, el cual establece un procedimiento claro para la identificación, clasificación y consolidación de los activos de información dentro del proceso de gestión de seguridad.

El segundo elemento es la *Matriz de Riesgos de Seguridad de la Información*, que define la hoja de ruta para la identificación, valoración y tratamiento adecuado de los riesgos asociados a los activos de información. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información y los datos institucionales, protegiendo los mismos ante posibles amenazas y vulnerabilidades.

8.1. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Un activo de información es todo recurso que posee valor para la entidad dentro de su entorno operativo y digital, y que por tanto requiere medidas adecuadas de protección. Estos activos pueden incluir documentos físicos o electrónicos, aplicaciones, bases de datos, personas que gestionan o administran información, equipos de tecnologías de la información, infraestructura asociada, servicios tercerizados que soportan los procesos institucionales, así como las credenciales de acceso utilizadas por los funcionarios para ingresar a las plataformas y sistemas institucionales.

Figura 14. *Pasos para la identificación y valoración de activos*



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

8.1.1. Paso 1. Listar los activos por cada proceso: Consiste en identificar y registrar todos los activos de información que soportan los procesos de la entidad. Este inventario debe incluir activos tecnológicos, documentales, humanos, físicos, digitales y servicios tercerizados. El objetivo es establecer una base completa que permita una gestión integral de la seguridad de la información.

8.1.2. Paso 2. Identificar el dueño y custodio de los activos: Se establece que cada activo debe tener un dueño, responsable de su adecuado uso, protección y disposición, así como un custodio, encargado de su administración operativa. Este paso asegura claridad en roles y responsabilidades, facilita el control y permite implementar medidas de seguridad acordes con el nivel de importancia y uso del activo.

8.1.3. Paso 3. Clasificar los activos por tipo: Se deben categorizar los activos según su naturaleza: hardware, software, información, servicios, infraestructura, personas, medios de almacenamiento, entre otros. Esta clasificación permite organizar el inventario, facilitar la valoración de riesgos y orientar las acciones de protección según la tipología del activo.

8.1.4. Paso 4. Clasificar la información: La información debe ser clasificada considerando criterios como confidencialidad, integridad y disponibilidad. Esta clasificación permite determinar las medidas de seguridad necesarias y garantizar que la información sea tratada de forma apropiada en función de su sensibilidad y valor institucional.

8.1.5. Paso 5. Determinar la criticidad del activo: La criticidad de los activos de información será establecida mediante la aplicación de la fórmula definida en la matriz institucional de valoración, la cual utiliza las variables de confidencialidad, integridad y disponibilidad obtenidas en el proceso de clasificación de la información.

El resultado de esta valoración determina de manera objetiva el nivel de importancia del activo para la continuidad de los procesos institucionales y el impacto potencial derivado de

su afectación. Este nivel de criticidad constituye un insumo obligatorio para priorizar los activos que requieren la implementación de controles y medidas de seguridad reforzadas dentro del proceso de gestión de riesgos de seguridad de la información.

8.1.6. Paso 6. Identificar si existe una Infraestructura Crítica Cibernética Nacional (ICCN): Se verifica si alguno de los activos identificados cumple criterios para ser considerado parte de una Infraestructura Crítica Cibernética Nacional, conforme a los lineamientos de seguridad digital del Estado. Si aplica, se deben implementar controles adicionales y mecanismos de monitoreo reforzado, dada su relevancia para el funcionamiento del país y la prestación de servicios esenciales.

8.2. MATRIZ DE INVENTARIO DE ACTIVOS DE INFORMACIÓN

Para la gestión sistemática de los activos de información incluidos en el alcance de la estrategia de gestión de riesgos de seguridad de la información, la entidad implementará un inventario que permita registrar de manera estructurada cada activo identificado. Los campos que se presentan a continuación son sugeridos por la Guía v7 del DAFP y pueden ser ajustados o adaptados según el contexto, necesidades y capacidades de la entidad:

- **Macroproceso:** Identificación del macroproceso institucional al que pertenece el activo de información, en caso de que la entidad cuente con esta estructura.
- **Proceso:** Proceso institucional al que está asociado el activo de información.
- **Identificador:** Código único sugerido para cada activo, construido, por ejemplo, mediante la concatenación del código de la dependencia según la Tabla de Retención Documental (TRD) y un número consecutivo.
- **Tipo de activo: Clasificación general del activo según su naturaleza, incluyendo:**
    - **Información y datos de la entidad:** Documentos físicos o electrónicos, bases de datos, contratos, manuales, procedimientos, planes de continuidad, acuerdos de confidencialidad y otros documentos institucionales.
    - **Sistemas de información y aplicaciones de software:** Software de aplicación, plataformas, interfaces, sistemas operativos y herramientas de desarrollo.
    - **Dispositivos de TI – Hardware:** Equipos de cómputo y otros dispositivos críticos para los procesos institucionales.
    - **Soportes de almacenamiento:** USB, discos duros, CDs, SAN, NAS u otros medios de almacenamiento físico o electrónico.
    - **Servicios:** Servicios de computación y comunicaciones, incluyendo Internet, intranet, directorios compartidos y otros servicios tecnológicos.
    - **Recursos humanos:** Personas cuya función impacta la gestión o custodia de la información.
    - **Instalaciones:** Espacios físicos que soportan la operación tecnológica o el resguardo de la información.
    - **Redes:** Infraestructura de comunicación y transmisión de datos.

- **Oficina:** Área, dependencia o proceso responsable de identificar el activo.
- **Serie documental:** Serie documental correspondiente al área, proceso o dependencia que identifica el activo.
- **Subserie documental:** Subserie asociada al activo de información según la dependencia o proceso responsable.
- **Nombre:** Denominación completa del activo de información.

- **Descripción:** Resumen claro que permita identificar el activo de información.
- **Responsable de la producción de la información (Propietario del activo):** Área, dependencia o proceso encargado de producir y generar el activo.
- **Fecha de generación de la información:** Fecha en la que el activo fue creado o incorporado al inventario/TRD.
- **Responsable de la información (Custodio del activo):** Área, dependencia o proceso encargado de la custodia, control y protección del activo.
- **Fecha de ingreso al archivo:** Fecha en que el activo ingresa al archivo de gestión.
- **Soporte de registro:**
  - Físico (análogo)
  - Digital (electrónico) — aplica para activos de tipo “Información”
  - N/A — para los demás tipos de activos

- **Medio de conservación:** Archivo institucional o instancia administrativa responsable de custodiar, organizar y proteger la información.
- **Formato:** Forma, tamaño o modo en que se presenta la información (ej. hoja de cálculo, imagen, audio, video, documento de texto, etc.).
- **Idioma:** Lengua o dialecto en que se encuentra la información.
- **Clasificación de activos por propiedad:**
  Confidencialidad, Integridad y Disponibilidad — cada propiedad se clasifica en tres niveles: Alta, Media o Baja, de acuerdo con criterios de valoración institucional.
- **Nivel de criticidad del activo:** Resultado de la sumatoria de la clasificación de propiedades, determinando si el activo es de criticidad Alta, Media o Baja.
- **Es Infraestructura Crítica Cibernética Nacional (ICCN):** Indica si el activo cumple con los criterios establecidos en los lineamientos del MSPI para infraestructuras críticas cibernéticas.
- **Información publicada: Indica si el activo está disponible públicamente, en intranet o internet, o no está publicado.**

  - Publicada (Interno – Intranet)
  - Publicada (Externo – Internet)
  - No publicada

- **Lugar de consulta o ubicación:** URL, sistema de información o ubicación física del activo.
- **Índice de información clasificada y reservada:**
  - **Objeto legítimo de la excepción:** Identificación de la excepción prevista en la Ley 1712 de 2014; si no aplica, se registra N/A.

  - **Fundamento constitucional o legal:** Norma que justifica la clasificación o reserva de la información.
  - **Fundamento jurídico de la excepción:** Norma específica que respalda la calificación.
  - **Excepción total o parcial:** Indica si la clasificación aplica a la totalidad o solo a partes del activo.
  - **Fecha de clasificación:** Fecha en la que se calificó la información como reservada o clasificada.
  - **Tiempo de clasificación:** Duración de la clasificación o reserva; clasificación ilimitada, reserva máximo 15 años.

- **Activos que contienen datos personales:**

  - ¿Contiene datos personales? (Sí/No)

- ¿Contiene datos de niños, niñas o adolescentes? (Sí/No)

- **Tipos de datos personales:**
  - Dato personal público
  - Dato personal privado
  - Dato semiprivado
  - N/A — si no aplica

- **Finalidad de la recolección:** Propósito de captura, almacenamiento y uso del dato en la entidad.
- **Autorización para el tratamiento de datos personales:** Indica si se cuenta con la autorización correspondiente (Sí/No).

- Matriz de Riesgos de Seguridad de la Información

Para cada activo de información identificado y clasificado según su criticidad, la entidad llevará a cabo el proceso de gestión de riesgos, registrando los resultados en la Matriz de Riesgos de Seguridad de la Información. Esta matriz permite consolidar, de manera estructurada, la información relacionada con amenazas, vulnerabilidades y riesgos, facilitando su análisis, tratamiento y seguimiento. Los campos y elementos que se incluyen en la matriz son recomendados por la Guía versión 7 del DAFP, y podrán adaptarse según el contexto y las necesidades de la entidad:

Campos de la Matriz de Riesgos

- ✓ Proceso: Proceso institucional al que está asociado el activo de información.
- ✓ Referencia: Número o código de referencia del activo en el inventario institucional.
- ✓ Activo de Información: Nombre del activo de información.
- ✓ Tipo de Activo: Clasificación del activo según su naturaleza, pudiendo incluir:
  - Información
  - Software
  - Hardware
  - Servicios
  - Intangibles
  - Infraestructura Crítica Cibernética Nacional (ICCN)
  - Recursos Humanos
  - Instalaciones y otros servicios

8.3. IDENTIFICACIÓN DE ÁREAS DE IMPACTO

Se define el área de impacto, entendida como la consecuencia negativa sobre los objetivos institucionales en caso de materialización de un riesgo o incidente de seguridad de la información, afectando la gestión y operación de la entidad.

8.4. IDENTIFICACIÓN DE FACTORES DE RIESGO

Los factores de riesgo corresponden a las fuentes generadoras de amenazas y vulnerabilidades que pueden afectar los activos de información:

- **Amenaza:** Evento potencial que podría generar un incidente no deseado, afectando sistemas, información o procesos (ISO/IEC 27001:2022).
- **Vulnerabilidad:** Debilidad o deficiencia en un activo o control que puede ser explotada por una amenaza (ISO/IEC 27001:2022).

8.5. DESCRIPCIÓN DEL RIESGO

Para cada riesgo identificado se registran:

- **Tipo de riesgo:** Clasificación según el efecto sobre la información:
    - Pérdida de Disponibilidad
    - Pérdida de Integridad
    - Pérdida de Confidencialidad

- **Descripción del riesgo:** Detalle de la situación que genera el riesgo.
- **Clasificación del riesgo:** Nombre o denominación del posible incidente de seguridad.

8.6. ANÁLISIS DE RIESGO INHERENTE

Se analiza la probabilidad y el impacto de que los riesgos se materialicen, considerando los criterios cuantitativos y cualitativos establecidos:

- **Probabilidad:** Evaluación de la frecuencia con la que podría materializarse el riesgo, expresada en:

Probabilidad	Frecuencia de la Actividad
Muy Baja 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta 80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

- **Impacto:** Medición del efecto económico o reputacional del riesgo, según rangos predefinidos:

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor 40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Mayor a 100 SMLMV y Menor a 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

Análisis de severidad

Se determina la **zona de riesgo inherente** en la matriz de calor, combinando probabilidad e impacto, para priorizar la atención y tratamiento de los riesgos.

8.7. DISEÑO Y ANÁLISIS DE CONTROLES

Para cada riesgo se definen los controles necesarios para su mitigación:

- **Número de control:** Consecutivo de los controles establecidos.
- **Control Anexo A:** Referencia a los controles de la norma ISO/IEC 27001:2022, pudiendo añadirse controles adicionales según las necesidades de la entidad.
- **Descripción del control:** Forma en que se implementará el control en la entidad, incluyendo aspectos técnicos y administrativos complementarios.

8.8. VALORACIÓN DE CONTROLES

Se evalúa cómo los controles afectan la **probabilidad o impacto** de los riesgos:

- **Afectación Probabilidad:** Indica si el control busca reducir la ocurrencia del riesgo.
- **Afectación Impacto:** Indica si el control busca disminuir el efecto del riesgo.
- **Atributos del control:** Se incluyen eficiencia, formalización, documentación, frecuencia, evidencia y fuente de ejecución (interna, externa o mixta).

8.9. VALORACIÓN DE RIESGO RESIDUAL

Tras la implementación de controles, se determina el **riesgo residual**, considerando la efectividad de los controles y su impacto sobre la probabilidad e impacto de cada riesgo.

Plan de implementación de controles:

Para cada control se define un plan de acción que incluye:

- **Tratamiento:** Estrategia para el riesgo (Reducir, Compartir, Aceptar o Evitar).
- **Plan de acción:** Identificación de las acciones para implementar el control.
- **Responsable:** Cargo o dependencia encargada de ejecutar el plan.
- **Fecha de implementación:** Plazo máximo para completar la acción.
- **Seguimiento:** Periodicidad de revisión del control implementado.
- **Estado:** Nivel de avance o cumplimiento del plan de implementación.

9. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA – SIGRIP

La Alcaldía de Bucaramanga adopta el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP en cumplimiento de la Ley 2195 de 2022, que establece la obligación de prevenir, gestionar y administrar los riesgos de corrupción, así como los relacionados con lavado de activos, financiación del terrorismo y proliferación de armas. En este marco, el SIGRIP fortalece la integridad institucional, la ética pública, la transparencia y la confianza ciudadana, articulándose con el Programa de Transparencia e Integridad Pública (PTEP), el Modelo Integrado de Planeación y Gestión – MIPG y la Gestión Integral de Riesgos institucional.

9.1. INTEGRIDAD PÚBLICA

La integridad pública es un principio esencial de la función administrativa y orienta la actuación ética, transparente, imparcial y responsable de los servidores públicos, contratistas y colaboradores de la Alcaldía de Bucaramanga.

En la entidad, la integridad promueve:

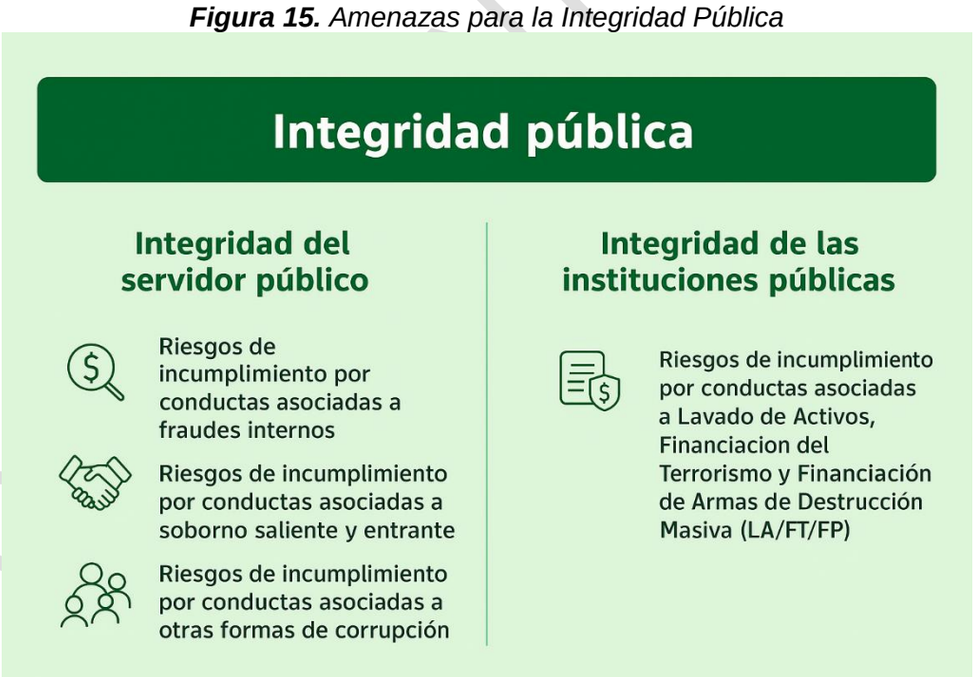
- La apropiación de los valores del servicio público.
- La integración de mecanismos y orientaciones que aseguren la idoneidad en la prestación del servicio.
- La apertura al diálogo con la ciudadanía
- Promoción de la cultura del autocontrol, la transparencia y la rendición de cuentas.

El SIGRIP refuerza estas prácticas al identificar, analizar y tratar los eventos que puedan comprometer la integridad institucional y afectar la confianza ciudadana. Sin embargo, además de promover una cultura de cumplimiento que consolide la legalidad, es necesario adoptar medidas que permitan gestionar las incertidumbres que puedan poner en riesgo la garantía del interés general, desarrolladas en los apartados siguientes:

9.2. AMENAZAS PARA LA INTEGRIDAD PÚBLICA

En coherencia con la Guía del DAFP versión 7, la Alcaldía identifica y administra las principales amenazas que pueden impactar la integridad institucional. Estas amenazas orientan el análisis y control de los riesgos de integridad pública dentro del SIGRIP, los cuales se presentan a continuación:

Figura 15. *Amenazas para la Integridad Pública*



Fuente: Secretaría de Transparencia, 2025

9.2.1. Soborno: Constituye una de las manifestaciones más recurrentes que afectan la integridad pública y se entiende como ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida, de cualquier valor —financiero o no financiero—, directa o indirectamente, con el fin de influir en la actuación de una persona para que realice u omita un acto en violación de la ley. En el marco del SIGRIP, el soborno puede presentarse en dos modalidades:

- **Soborno Entrante:** cuando un servidor público acepta o solicita una ventaja indebida ofrecida por una contraparte externa para favorecer intereses particulares.

- **Soborno Saliente:** cuando un servidor público, en nombre de la entidad, ofrece, promete o entrega una ventaja indebida a un tercero para obtener un beneficio o influir en decisiones externas.

En la entidad se gestiona mediante:

- Segregación de funciones
- Trazabilidad de decisiones,
- Controles en contratación, trámites y servicios,
- Mecanismos de denuncia y protección al denunciante.

9.2.2. Fraude. Corresponde a acciones u omisiones intencionales que buscan obtener un beneficio indebido para sí o para terceros, mediante la manipulación, alteración, ocultamiento o falsificación de información, documentos, transacciones o decisiones administrativas.

En el SIGRIP, el fraude debe ser identificado como un riesgo independiente, dado su potencial para generar afectaciones económicas, operativas y reputacionales a la Alcaldía de Bucaramanga.

En la entidad, su control se refuerza con:

- Verificaciones documentales
- Controles tecnológicos
- Supervisión contractual
- Auditorías internas
- Fortalecimiento del MSPI.

9.2.3. Inadecuada Gestión del Conflicto de Intereses. Se presenta cuando los intereses personales de una servidora o servidor pueden influir o aparentar influir en sus decisiones. La inadecuada gestión ocurre cuando el conflicto no se declara, no se tramita o se permite que afecte la imparcialidad, generando riesgos de favorecimiento, parcialidad o afectación al interés general. En el SIGRIP se considera un riesgo relevante especialmente en actividades como contratación, trámites, decisiones y supervisión.

La Alcaldía fortalece su administración mediante:

- Declaraciones de conflicto de interés
- Reglas de abstención y reemplazo (garantizan que el servidor involucrado se aparte del trámite y que otro funcionario asuma temporalmente la actuación)
- Controles de transparencia
- Registro de situaciones que puedan afectar la objetividad en decisiones.

9.2.4. Corrupción: Comprende acciones que desvían la función o los recursos públicos para obtener beneficio propio o para un tercero. Incluye favorecimientos indebidos, direccionamiento de decisiones, abuso de funciones y otras prácticas que comprometen la integridad institucional. Esas conductas incluyen: Uso del poder para obtener beneficios personales, Pérdida o disminución del patrimonio público, Perjuicio social significativo y corrupción electoral. Es la principal amenaza para la integridad pública y debe gestionarse mediante un enfoque preventivo y coherente con el SIGRIP.

Se gestiona mediante:

- Aplicación del SIGRIP
- Monitoreo del PTEP
- Fortalecimiento de controles en procesos críticos
- Mecanismos de control preventivo y disciplinario
- Participación ciudadana y transparencia activa.

9.2.5. Lavado de Activos (LA), Financiación del Terrorismo (FT) y Proliferación de Armas (FP): Se presenta cuando terceros buscan utilizar la entidad para legitimar recursos ilícitos o canalizar fondos hacia actividades ilegales. Este riesgo puede aparecer en pagos, contratos, operaciones y relacionamiento con contrapartes. El SIGRIP busca identificar puntos de riesgo, aplicar debida diligencia, monitorear operaciones inusuales y reportar sospechas a las autoridades. Las medidas incluyen:

- Consulta de listas restrictivas (bases de datos oficiales que contienen personas o entidades sancionadas, inhabilitadas o vinculadas a actividades ilegales)
- Verificación de antecedentes de contratistas y proveedores
- Alertas en procesos administrativos sensibles
- Reportes a la Unidad de Información y Análisis Financiero -UIAF cuando corresponda
- Fortalecimiento de la debida diligencia.

9.3. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA – SIGRIP

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP de la Alcaldía de Bucaramanga se fundamenta en un enfoque integral que articula los riesgos de gestión, fiscales y de seguridad de la información con los riesgos de integridad pública, en cumplimiento de la Ley 2195 de 2022, la Guía de Gestión Integral del Riesgo y Diseño de Controles – Versión 7 del DAFP y el Programa de Transparencia e Integridad Pública (PTEP). Este sistema reconoce que amenazas como el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y los riesgos LA/FT/FP pueden constituir causas de riesgos institucionales que impacten la operación, la transparencia y la confianza ciudadana.

El SIGRIP comprende un conjunto de elementos interrelacionados que permiten gestionar de manera estructurada los riesgos de integridad pública, tales como:

1. Política de Gestión Integral de Riesgos;
2. Debida diligencia en el conocimiento de contrapartes
3. Función de cumplimiento en materia de integridad y
4. Herramientas de gestión y control orientadas a prevenir, detectar y mitigar conductas que afecten la probidad institucional.

Para su adecuada operación, el SIGRIP incorpora un análisis ampliado del contexto organizacional que contempla la estructura y funciones de la Administración Municipal, los grupos de valor y contrapartes, la naturaleza y complejidad de los procesos y servicios, las interacciones institucionales, la gestión contractual y las obligaciones legales y administrativas de la entidad. Este análisis orienta la identificación de vulnerabilidades, puntos críticos y condiciones que pueden favorecer la materialización de riesgos de integridad.

Por otra parte, el **liderazgo** del SIGRIP se desarrolla bajo el esquema de líneas de defensa y los roles, garantizando la responsabilidad compartida y supervisión independiente (Tabla 3).

La planificación del SIGRIP se integra con los lineamientos de la Política de Gestión Integral de Riesgos e incluye la definición del objetivo, alcance, niveles de riesgo aceptados

y metodología institucional. **Su operación** se basa en la adopción de controles, la debida diligencia, la función de cumplimiento y el monitoreo permanente, garantizando que la gestión pública se realice en pleno cumplimiento de la ley, fortaleciendo la transparencia, la integridad y la confianza ciudadana.

9.4. METODOLOGÍA PARA LA IDENTIFICACIÓN Y VALORACIÓN DE LOS RIESGOS PARA LA INTEGRIDAD PÚBLICA

La Alcaldía de Bucaramanga identifica y valora los riesgos para la integridad pública (soborno, fraude, conflicto de intereses, corrupción y LA/FT/FP) aplicando la misma metodología institucional definida para la Gestión Integral del Riesgo, complementada con los criterios específicos establecidos en el SIGRIP. Esto garantiza coherencia metodológica y un análisis integral de todos los riesgos institucionales.

Figura 16. *Sistema de Gestión de Riesgos para la Integridad Pública*

Fuente: Secretaría de Transparencia de la Presidencia de la República, 2025.

La metodología respecto a los riesgos para la integridad pública se desarrolla en cuatro pasos:

9.4.1. Paso 1. Identificación y descripción del riesgo

a. Identificación de puntos de riesgo:

- Para LA/FT/FP se analizan operaciones que impliquen intercambio de recursos (pagos, recaudos, contratación, subsidios).
- Para soborno, fraude, conflicto de intereses y corrupción, el riesgo puede presentarse en cualquier actividad del proceso y no solo las operaciones.

b. Identificación del impacto: Además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

Las **consecuencias legales** se originan cuando existe incumplimiento normativo u obligaciones que pueden derivar en sanciones, procesos judiciales o administrativos. Por su parte, **el contagio** ocurre cuando riesgos de integridad materializados en partes relacionadas —aunque no vinculadas directamente con la entidad— generan impactos económicos, reputacionales o legales. Tanto las consecuencias legales como las de contagio deben valorarse como afectación económica, siguiendo los criterios del numeral 6.2, tabla 8.

c. Identificación de factores de riesgo: Se analizan las contrapartes, productos, canales y jurisdicciones, que en conjunto conforman una “transacción u operación”, entendida como cualquier intercambio de bienes o servicios entre la Alcaldía y un tercero. Estos factores permiten detectar señales de alerta, operaciones inusuales y riesgos de LA/FT/FP que deben gestionarse oportunamente. Tabla 5 de “Factores de Riesgo” definida en el numeral 6.1.3 de la presente política.

d. **Descripción del riesgo:** Se usa la misma fórmula definida en la figura 6 de esta política:

“Posibilidad de [impacto] por [causa inmediata] en [actividad], a causa de [causa raíz]”

Las causas inmediatas de los riesgos para la integridad pública incluyen soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción y riesgos de LA/FT/FP. Estas amenazas, descritas en el numeral 9.2, son la base para identificar y analizar los riesgos asociados.

Tabla 14. *Ejemplos como referente para análisis del riesgo*

Impacto	Causa inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]”.	
	Soborno saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una Impacto Causa inmediata Causa raíz persona actúe o se abstenga de actuar […]”.	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	
Económico, Reputacional, Legal, Operativo o de Contagio	Riesgos LA/FT/FP	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva	Descripción de la Operación o Transacción

Fuente: Secretaría de Transparencia de la Presidencia de la República, 2025

De acuerdo con la metodología establecida en el numeral 6.1.4, los riesgos y sus causas inmediatas pueden formularse de la siguiente manera:

***Tabla 15**. Ejemplos descripción de riesgos de integridad*

Riesgo	Descripción del riesgo
Corrupción	*Posibilidad de afectación económica por corrupción* en la evaluación de procesos de selección, debido al direccionamiento o favorecimiento hacia un proponente específico.
Fraude interno	*Posibilidad de afectación económica por fraude interno* en la asignación de subsidios, a causa de errores u omisiones realizadas para beneficio personal o de terceros.
Soborno saliente	*Posibilidad de afectación reputacional por soborno saliente* en el seguimiento a la agenda legislativa, debido al ofrecimiento indebido de incentivos para influir en decisiones a favor de la entidad.
Soborno entrante	*Posibilidad de afectación reputacional por soborno entrante* al aceptar o solicitar ventajas indebidas en la asignación de citas, mediante manipulación del sistema de información.
Conflicto de intereses	*Posibilidad de afectación económica por conflicto de interés* no declarado o no gestionado, derivado de decisiones tomadas en el comité de contratación donde el servidor tiene un interés particular.
Riesgos LA/FT/FP	*Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva,* a causa de fallas en las operaciones de pago de subsidios.
	Posibilidad de contagio por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de contratación directa.
	Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de recaudo.

Fuente: Función Pública, 2025

9.4.2. Paso 2. Análisis del Riesgo Inherente: Se aplica la metodología institucional para valorar probabilidad e impacto, siguiendo los criterios establecidos en el capítulo metodológico de la Política. El análisis debe reflejar que los riesgos para la integridad requieren especial atención por su naturaleza y obligatoriedad de prevenir, detectar y reportar.

Para el cálculo de probabilidad e impacto, aplica lo establecido en el Capítulo VI de la presente política, específicamente en el numeral 6.2, con las correspondientes Tablas 7 y 8.

9.4.3. Paso 3. Diseño y análisis de controles: Los controles deben quedar registrados en la matriz y ser consistentes con el MIPG y el MECI. Los riesgos de integridad se controlan mediante:

- Controles preventivos, detectivos y correctivos.

- Procedimientos específicos del SIGRIP: debida diligencia, función de cumplimiento y herramientas de gestión.
- Lineamientos del Programa de Transparencia e Integridad.

El diseño y análisis de controles, están definidos en el Capítulo VI de esta política, específicamente en lo definido en el numeral 6.3 que establece la estructura general, los atributos y tablas para su valoración.

9.4.4. Paso 4. Valoración del riesgo residual: Se determina el nivel de riesgo posterior a la aplicación de controles, aplicando la misma escala definida en el Capítulo VI de la presente política.

El resultado de esta metodología permite que la Alcaldía:

- Integre los riesgos de integridad a la gestión institucional del riesgo.
- Aplique criterios homogéneos y comprensibles.
- Identifique eventos críticos sin necesidad de procesos complejos.
- Facilite la formulación de riesgos por parte de los líderes de proceso.

9.5. HERRAMIENTAS DE GESTIÓN DEL RIESGO PARA LA INTEGRIDAD PÚBLICA

Para asegurar la operación efectiva del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, la Alcaldía de Bucaramanga además de contar con la Política para la gestión integral de riesgos, adoptará un conjunto de herramientas para fortalecer la prevención, detección y respuesta frente a los riesgos de soborno, fraude, conflicto de intereses, corrupción y LA/FT/FP:

9.5.1. Debida Diligencia: La alcaldía de Bucaramanga aplicará mecanismos de debida diligencia para el conocimiento de sus contrapartes conforme a la Ley 2195 de 2022, con el fin de identificar beneficiarios finales, verificar su identidad y reputación, y prevenir riesgos de integridad como soborno, fraude, conflicto de intereses, corrupción y LA/FT/FPADM. Estos mecanismos se aplicarán antes de iniciar la relación y durante su ejecución, con un enfoque de razonabilidad y proporcionalidad mediante esquemas de debida diligencia simplificada, estándar o ampliada según el nivel de riesgo.

Para tal fin, la entidad contará con un **Manual de Debida Diligencia**, que establecerá los lineamientos para la recolección, verificación y análisis de información; la consulta de fuentes oficiales como SIBOR, SIRI, antecedentes y listas restrictivas; la identificación de beneficiarios finales; la documentación y custodia de la información; los criterios para adoptar decisiones y controles derivados de los resultados; y el procedimiento para reportar operaciones inusuales o sospechosas a las autoridades competentes. Este manual será de obligatorio cumplimiento para los procesos en los que exista exposición a riesgos para la integridad pública.

9.5.2. Función de Cumplimiento: La entidad contará con una Función de Cumplimiento, asignada a una persona, grupo o dependencia, encargada de promover, verificar y fortalecer la implementación del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP. Esta función orientará a los líderes de proceso en la identificación, análisis y control de los riesgos de integridad, supervisará la correcta aplicación de la debida diligencia y evaluará periódicamente la efectividad del sistema, reportando sus resultados a la Alta Dirección. La función de cumplimiento no sustituye, elimina o restringe las funciones propias de las unidades de control interno.

Además, la gestión para la integridad pública requiere que se implemente una serie de políticas, procedimientos y códigos de conducta, que contribuyen a la integralidad del sistema.

a. Política ALA/CFT/CFP: La Alcaldía adoptará una Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Proliferación de Armas (ALA/CFT/CFP), que:

- Formaliza el compromiso de la Alta Dirección con la prevención de LA/FT/FP.
- Prohíbe expresamente cualquier conducta asociada a estos riesgos.
- Ordena la aplicación de la debida diligencia a todas las contrapartes.
- Exige el cumplimiento estricto de la normativa vigente.
- Promueve la denuncia segura mediante los canales institucionales.
- Establece consecuencias en caso de incumplimiento.

b. Política Antisoborno: La entidad prohíbe cualquier acto de soborno u ofrecimiento de beneficios indebidos. La Alta Dirección reafirma su compromiso con la integridad y la transparencia, promoviendo la denuncia de conductas sospechosas y aplicando sanciones cuando corresponda.

Incluye:
- Definición y prohibición expresa de cualquier forma de soborno entrante o saliente.
- Obligación institucional de prevenir, detectar y reportar señales de alerta.
- Compromiso de la Alta Dirección con una cultura de integridad y transparencia.

c. Política Antifraude: La Alcaldía rechaza todo tipo de fraude y establece controles para prevenirlo y detectarlo. Todo servidor o contratista debe reportar comportamientos irregulares y cumplir con los lineamientos de transparencia y legalidad.

Define:
- Conductas constitutivas de fraude interno o externo.
- Prohibición de prácticas fraudulentas en la gestión de recursos y decisiones administrativas.
- Lineamientos para su prevención y denuncia oportuna.

d. Procedimiento para la Gestión de Conflictos de Intereses: La entidad contará con un procedimiento para identificar, declarar y gestionar los conflictos de interés. Incluye ruta de declaración, revisión, tratamiento y seguimiento conforme a la normativa vigente. El procedimiento institucional deberá:

- Incluir situaciones típicas que generan conflicto de interés.
- Establecer el paso a paso para declarar, revisar y gestionar conflictos.
- Determinar acciones preventivas y correctivas.
- Verificar el cumplimiento de las declaraciones obligatorias.

e. Procedimiento para el Reporte de Operaciones Sospechosas: Se adoptará un procedimiento para identificar señales de alerta, reportarlas a la función de cumplimiento y, cuando corresponda, a la UIAF o autoridades competentes, garantizando confidencialidad y oportunidad.

f. Procedimiento del Canal de Denuncias Institucional: La Alcaldía contará con un procedimiento articulado al SIGRIP, que fortalecerá el canal de denuncias mediante lineamientos claros para recibir, evaluar y tramitar reportes relacionados con riesgos de integridad. Incluye:

- Medios habilitados para recibir denuncias e inquietudes.
- Evaluación y clasificación de los reportes.
- Acciones de tratamiento y seguimiento.
- Cierre documentado del trámite conforme a la normativa vigente.

Todas las herramientas —políticas, procedimientos y manuales— harán parte del Programa de Transparencia y Ética Pública-PTEP, asegurando coherencia con el MIPG y con los lineamientos del DAFP y la Secretaría de Transparencia.

9.5.3. Monitoreo, evaluación, auditoría y mejora del SIGRIP: La Alcaldía de Bucaramanga garantizará que el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP sea objeto permanente de monitoreo, evaluación, auditoría y mejora continua, conforme al esquema de líneas de defensa del MIPG y al MECI.

- **Monitoreo (Primera línea de defensa):** Los líderes de proceso, junto con sus equipos, realizarán el seguimiento periódico al estado de los riesgos asociados a la integridad pública, generando los reportes definidos en la Política de Gestión Integral de Riesgos y remitiéndolos al Administrador del SIGRIP.

- **Evaluación (Segunda línea de defensa):** El Administrador del Programa de Transparencia evaluará el cumplimiento de los objetivos del SIGRIP, analizará los resultados del monitoreo y consolidará los informes con base en los indicadores definidos para la gestión del riesgo de integridad.

- **Auditoría (Tercera línea de defensa):** La Oficina de Control Interno efectuará auditorías independientes al SIGRIP para verificar su conformidad, eficacia y el funcionamiento de sus controles, de acuerdo con el plan anual de auditoría y bajo un enfoque basado en riesgos.

- **Mejora continua (Línea estratégica):** La Alta Dirección revisará de manera periódica la operación del SIGRIP y adoptará las acciones de mejora que resulten de los hallazgos del monitoreo, las evaluaciones y las auditorías, asegurando la actualización permanente del sistema y su contribución al fortalecimiento de la integridad pública.

10. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

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

Tabla 16. *Acciones de respuesta a riesgos materializados*

Tipo de Riesgo	Responsable	Acciones de Respuesta Actualizadas (V10 – SIGRIP)
Riesgos de Integridad Pública (Corrupción, Soborno Entrante/Saliente, Fraude, Conflicto de Intereses, LA/FT/FP)	**Líder del Proceso** (Primera línea)	• Notificar de inmediato al Proceso de Planeación y Direccionamiento Estratégico (segunda línea). • Activar medidas de contención para proteger la operación, la continuidad del servicio y la evidencia. • Aplicar lineamientos del SIGRIP: verificación de contrapartes, señales de alerta, consulta de listas restrictivas si aplica. • Documentar acciones correctivas y preventivas en el Plan de Mejoramiento. • Actualizar el mapa de riesgos del proceso. • Avanzar en el conducto regular para denuncias ante autoridad competente, cuando corresponda.

	Oficina de Control Interno (Tercera línea)	• Notificar al líder del proceso y requerir acciones inmediatas. • Verificar activación del SIGRIP y la trazabilidad del caso. • Informar a la segunda línea para ajustes y actualización del mapa. • Realizar auditoría o seguimiento independiente al caso.
Riesgos de Gestión y Seguridad de la Información (Zona Extrema, Alta y Moderada)	**Líder del Proceso**	• Activar planes de contingencia o tratamiento de incidentes para asegurar continuidad o restablecimiento del servicio. • Analizar causas y definir acciones preventivas y correctivas en el Plan de Mejoramiento Institucional. • Actualizar el mapa de riesgos del proceso. • Informar al Proceso de Planeación y Direccionamiento Estratégico sobre el hallazgo.
	Oficina de Control Interno	• Informar al líder del proceso sobre el hecho. • Notificar a la segunda línea. • Acompañar la revisión de riesgos y verificar acciones tomadas. • Confirmar actualización del mapa de riesgos correspondiente.
Riesgos de Gestión y Seguridad de la Información (Zona Baja)	**Líder del Proceso**	• Revisar el hecho y aplicar correctivos mínimos necesarios. • Actualizar el mapa de riesgos si aplica.
	Oficina de Control Interno	• Verificar acciones tomadas y cierre del caso. • Informar a la segunda línea si se requiere ajuste metodológico.

Fuente: Secretaría de Planeación

11. COMUNICACIÓN Y SOCIALIZACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Política para la Gestión Integral de Riesgos y los Mapas de Riesgos Integrales serán comunicados y socializados a todos los servidores públicos y contratistas de la Alcaldía de Bucaramanga mediante los diferentes canales institucionales disponibles.

La gestión del riesgo constituye un componente esencial para el fortalecimiento de la integridad, la transparencia y la eficiencia administrativa; por ello, la Entidad desarrollará jornadas de socialización internas y externas que aseguren el conocimiento, comprensión y correcta aplicación de los lineamientos definidos en la Política versión 10 y en el SIGRIP.

De igual manera, se promoverá que los líderes de proceso fortalezcan sus capacidades conceptuales y operativas en materia de gestión integral del riesgo, de forma que puedan orientar adecuadamente a sus equipos y garantizar la implementación efectiva de la política en cada uno de los procesos institucionales.

12. MONITOREO Y SEGUIMIENTO INTEGRAL

12.1. MONITOREO Y SEGUIMIENTO

Los líderes de proceso en conjunto con su equipo de trabajo deben registrar los avances en el Mapa Integral 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.

12.1.1 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).

12.1.2 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 Integral 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 Integral de Riesgos en la página web de la entidad.
- Seguimiento a la gestión a integridad de riesgos
- 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