2026

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

ALCALDÍA DE BUCARAMANGA

Instituto de Empleo y Fomento Empresarial

IMEBU

Versión 3.0

POLITICA DE ADMINISTRACIÓN DEL RIESGO

INSTITUTO DE EMPLEO Y FOMENTO EMPRESARIAL

Cargo del Líder Estratégico	Proceso que produce el documento
Dirección **Subdirección Administrativa y Financiera.** **Subdirección Técnica.**	**Gestión de Planeación Estratégico**

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE CAMBIOS**	**RESPONSABLE**
1.0	28/09/2023	Emisión Inicial del Documento	Apoyo Profesional MIPG
2.0	28/05/2025	Actualización del Documento	Apoyo Profesional MIPG
3.0	03-06-2026	Actualización integral de la Política de Administración del Riesgo. Se realizó la conversión del documento a formato editable y se efectuaron ajustes en su contenido. Se actualizó el marco normativo conforme a la versión 7 de la Guía para la Administración del Riesgo del DAFP (agosto de 2025). Asimismo, se modificó la clasificación de los riesgos de acuerdo con el Mapa de Riesgos de Gestión Institucional diseñado en mayo de 2026. Se ajustaron las estrategias para combatir el riesgo (planes de acción) conforme al nuevo Mapa Institucional de Riesgos de Gestión 2026 y se actualizó el esquema de seguimiento a los mapas de riesgos y controles.	Apoyo Profesional MIPG

Nota: El control de cambios en el documento, se refiere a cualquier ajuste que se efectúe sobre el documento.

Si la aprobación se realizó mediante acta de alguno de los comités internos, por favor especificar acta y mes del desarrollo de esta, en la columna "*Descripción de Cambios"*

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en las carpetas del SGC de IMEBU

TABLA DE CONTENIDO

INTRODUCCIÓN

En cumplimiento con lo establecido por el Departamento Administrativo de la Función Pública en la Guía Administración del Riesgo y el Diseño de controles en entidades públicas y el Modelo de Planeación y Gestión (MIPG), se da a conocer la política de Administración del Riesgo del Instituto Municipal de Empleo y Fomento Empresarial de Bucaramanga IMEBU.

En la vigencia actual, el IMEBU actualizó de manera colaborativa la Política de Administración de Riesgos con el fin de establecer el marco general de actuación de todos los servidores públicos de la entidad para la adecuada gestión de los riesgos mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales.

La política de administración del riesgo del IMEBU denota el grado de compromiso de la entidad frente al cumplimiento de los objetivos estratégicos y del plan de acción institucional, direccionando a los procesos a asumir un pensamiento basado en riesgos, que permita anticiparse, disminuir y contrarrestar el impacto de eventos inesperados.

Para el Instituto Municipal de Empleo y Fomento Empresarial de Bucaramanga es de gran importancia el cumplimiento de sus objetivos misionales a través del diseño e implementación de acciones soportadas en la prevención de los riesgos, a través de controles que promuevan la generación de comportamientos éticos y conlleven a la construcción de una cultura de buen gobierno, que impida la materialización de riesgos de gestión, corrupción, fiscales y seguridad de la información.

Con la presente Política, el IMEBU deja documentados los lineamientos de la gestión de los riesgos, junto con la descripción conceptual, orientación estratégica y el desarrollo operativo, con el fin de lograr el cumplimiento de los objetivos establecidos.

1. OBJETIVO

Establecer los lineamientos y criterios que orienten al Instituto Municipal de Empleo y Fomento Empresarial de Bucaramanga en la correcta identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos, fortaleciendo la cultura del control y la capacidad de alcanzar los objetivos institucionales.

2. ALCANCE

La Política de Administración de Riesgos aplica a todos los procesos (Gestión de Planeación Estratégica, Gestión de Planeación Presupuestal, Gestión de Calidad y Mejora Continua, Gestión Técnica para Emprendimiento, Gestión Técnica para Fortalecimiento Empresarial, Gestión Técnica para Fomento de Empleo, Gestión Jurídica, Gestión Financiera, Gestión del Talento Humano y SST, Gestión Informática, Gestión Documental, Gestión Recursos Físicos, Gestión de Comunicaciones, Gestión de Control Interno), conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso.

3. MARCO CONCEPTUAL

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital - Decreto Único TIC 1078 de 2015.
- **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.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **CICCI:** Comité Institucional de Coordinación de Control Interno.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Efectos 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.
- **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.
- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado, que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la correcta y adecuada adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes.
- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que

este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad - Impacto.

- **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.
- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, que transforma elementos de entrada en elementos de salida para generar un valor.
- **Plan Anticorrupción y de Atención al Ciudadano - PAAC:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Tolerancia al riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. • Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000), Ley 1581 del 2012 – protección de datos personales.
- **Riesgo Fiscal:** Es el efecto dañoso sobre los recursos públicos y/o bienes y/o intereses patrimoniales, de naturaleza publica, a causa de un evento potencial.
- **Riesgo inherente:** nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. MARCO NORMATIVO

- *Decreto 1499 de 2017, Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 – Modelo Integrado de Planeación y Gestión MIPG.*

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

- Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 – 2025.

- Norma Internacional ISO 31000 - 2018 – Proporciona Principios y Directrices para la Gestión del Riesgo.

- Ley 2195 de 2022 – Medidas en materia de Transparencia, Prevención y Lucha Contra la Corrupción.

- Ley 1581 del 2012 – Protección de Datos Personales en Colombia.

- Decreto 1072 de 2015 - Decreto Único Reglamentario del Sector Trabajo en Colombia.
- Resolución 0312 de 2019 – Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo.

5. POLITICA DE ADMINISTRACIÓN DEL RIESGO

La Alta dirección del IMEBU se compromete a identificar y a gestionar los riesgos a los cuales están expuestos y que pueden interferir al cumplimiento de su misión, visión, objetivos y planes estratégicos, definiendo medidas de control para prevenir su materialización y mitigar las posibles consecuencias a fin de mantener los niveles de riesgos aceptables, alineado a los requisitos legales aplicables.

6. RESPONSABILIDADES

En articulación con el Modelo Integrado de Planeación y Gestión - MIPG y la dimensión 7 de Control Interno, a continuación, se relaciona los niveles de responsabilidad y autoridad establecidos para la administración del riesgo determinados por las líneas de defensa:

6.1 Línea Estratégica

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Estratégica	Dirección General Comité Institucional de Control Interno	• Establecer y aprobar la Política de Administración del Riesgo y su actualización. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la Entidad y que puedan generar cambios en la estructura de riesgos y controles. Analizar los riesgos y amenazas institucionales que pueden afectar el cumplimiento de los planes estratégicos • Evaluar el estado del sistema de control interno y aprobar las modificaciones actualizaciones y acciones de fortalecimiento de este.

6.2 Primera Línea de Defensa

La primera línea de defensa en la política se refiere a los Controles por parte de los líderes de proceso y sus equipos. En esta línea se tiene como tarea fundamental el mantenimiento efectivo de controles internos, la ejecución procedimientos de riesgo y el control sobre la base del día a día. Es por ello que la gestión operacional identifica, evalúa, controla y mitiga los riesgos. Las responsabilidades de la primera línea de defensa son las siguientes:

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Primera línea de defensa	Líderes de Proceso y equipo de trabajo	• Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera, con énfasis en la prevención del daño antijurídico. • Definir, aplicar y hacer monitoreo a los controles para mitigar los riesgos identificados, alineado con las metas y objetivos de la Entidad y proponer mejoras a la gestión del riesgo en su proceso.

		• Supervisar la ejecución de los controles aplicados por el equipo de trabajo, detectarlas deficiencias de los controles y determinar las acciones de mejora a que haya lugar. Informar a la de Subdirección Técnica (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo • Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.

6.3 Segunda línea de defensa

La segunda línea de defensa está compuesta por la Media y Alta Gerencia, como son los jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, comités de riesgos (donde existan), áreas financieras, entre otros; que generen información para el aseguramiento de la operación. La responsabilidad de la segunda línea de defensa se centra en asegurar que los controles y procesos de gestión del riesgo de la primera línea de defensa sean apropiados y funcionen correctamente, supervisando la implementación de prácticas de gestión de riesgo eficaces.

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Segunda Línea de defensa	Subdirección Administrativa y Financiera Subdirección técnica Asesor Oficina Jurídica Profesional de Sistemas Comités Institucionales	• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. Participar en los ejercicios de autoevaluación. • Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. • Adoptar un esquema de Cobertura del Riesgo en los Procesos de Contratación de la entidad conforme a las directrices de Colombia Compra Eficiente.

Las responsabilidades aquí señaladas estarán sujetas al esquema de riesgos parametrizados en el Mapa de Riesgos de Gestión Institucional, también serán responsables los profesionales y apoyo a la gestión contratistas adscritos a cada dependencia.

6.4 Tercera línea de defensa

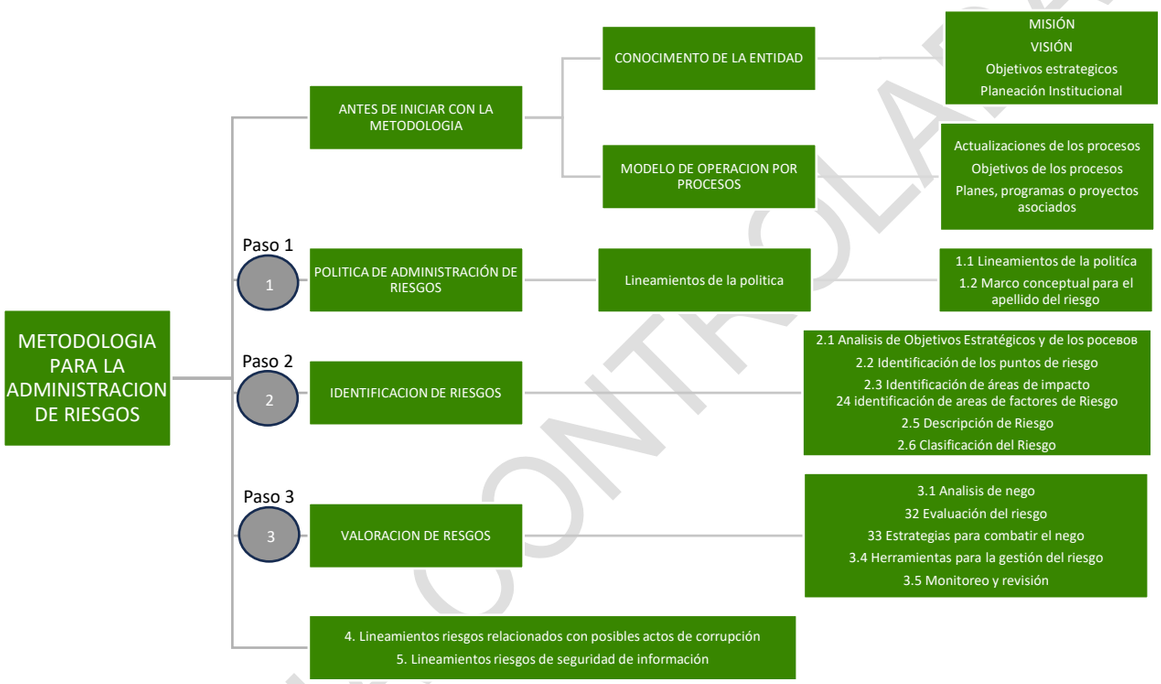
A cargo de Control Interno, la función de la auditoría interna a través de un enfoque basado en el riesgo proporcionará aseguramiento objetivo e independiente sobre la eficacia de gestión de riesgos y van incluidas las maneras en que funciona la primera y segunda línea de defensa.

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Tercera Línea de defensa	Control Interno	• 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 el mapa de riesgos de gestión, mapa de riesgos de corrupción (según la norma) de conformidad con el Plan Anual de Auditoría. • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.

7. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

La Metodología de Administración de Riesgos del IMEBU se ha diseñado según las especificaciones contenidas en la "Guía para la Gestión Integral del Riesgo en entidades Públicas " Versión 7 del DAFP de agosto de 2025. Lo anterior, siguiendo el siguiente esquema:

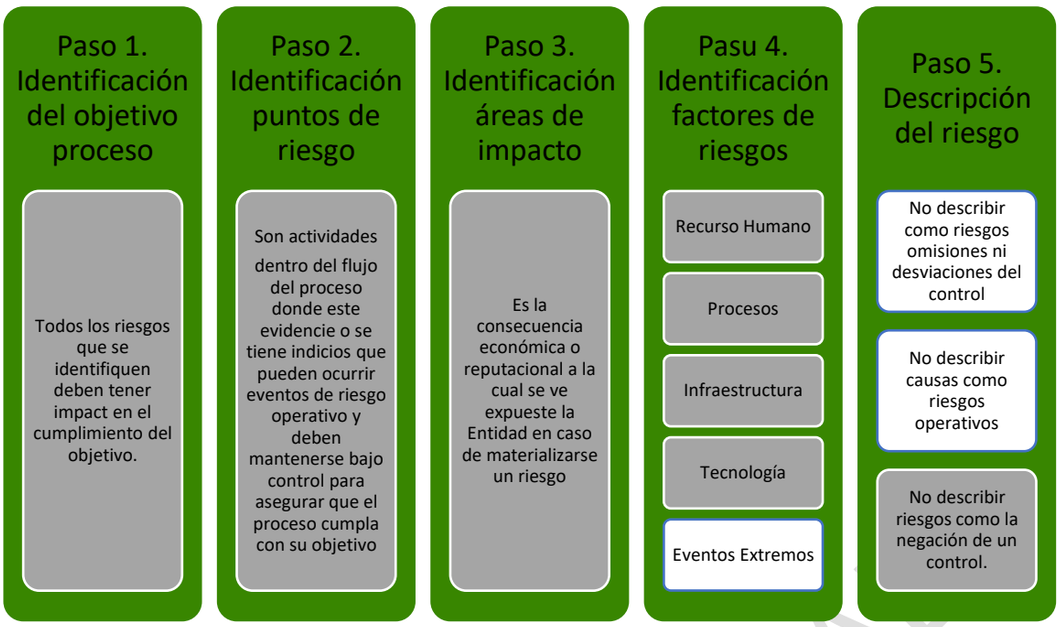


Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño institucional de Función Pública 2020

La metodología para la identificación y valoración de los riesgos variará teniendo en cuenta las particularidades de los riesgos de gestión, corrupción, seguridad de la información y fiscal.

8. IDENTIFICACIÓN DE RIESGOS

Tiene como objetivo identificar los riesgos que estén o no bajo el control de la entidad, para ello se debe tener en cuenta el contexto estratégico en el que opera la organización, la estructura orgánica de la administración central, las funciones primarias y secundarias de las dependencias, el objetivo del proceso y el análisis a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Para esta etapa se deberán tener en cuenta los siguientes pasos:



El paso inicial es la realización del análisis de los objetivos estratégicos del proceso y ajustar el objetivo del proceso cuando sea necesario, que se encuentren alineados con la misión y la visión institucional. Los objetivos deben incluir el qué, cómo, para qué, cuándo y cuánto.

Análisis de objetivos estratégicos y de los procesos	
CONTEXTO EXTERNO	Económicos (Disponibilidad de capital, liquidez, mercados, financieros, desempleo, competencia).
	Políticos (Cambios de gobierno, legislación, políticas públicas, regulación).
	Sociales (Demografía, responsabilidad social, orden público)
	Tecnológicos (Avances en tecnología, acceso a sistemas de información externos, Gobierno Digital).
	Medio Ambientales (Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible).
	Comunicación externa (Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad).
CONTEXTO INTERNO	Financieros (Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada).
	Personal (Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional).
	Procesos (Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del CONTEXTO conocimiento).
	Tecnología (Integridad y Seguridad de los datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información).
	Estratégicos (Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo).
	Comunicación interna (Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones).
CONTEXTO INTERNO DEL PROCESO	Diseño del proceso (Claridad en la descripción del alcance y objetivo del proceso). Interacciones con otros procesos (Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes).
	Procedimientos asociados (Pertinencia en los procedimientos que desarrollan los procesos).
	Responsables del proceso (Grado de autoridad y responsabilidad de los funcionarios frente al proceso).
	Comunicación entre los procesos (Efectividad en los flujos de información determinados en la interacción de los procesos).

También se deben tener en cuenta los puntos de riesgo, es decir las actividades donde pueden ocurrir eventos operativos de incertidumbre que deben estar controlados para asegurar el cumplimiento de los objetivos de cada uno de los procesos y los objetivos estratégicos.

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

Afectación Reputacional: es el deterioro de la relación con los grupos de interés como resultado de una percepción negativa sobre el comportamiento de la empresa.

- Perdidas por la disminución de la confianza en la integridad de la entidad que surge cuando su buen nombre es afectado.
- Opinión publica negativa sobre el servicio prestado.
- La afectación reputacional puede derivar en acciones que fomenten la creación de una mala imagen o un posicionamiento negativo en la mente de los ciudadanos.

Factores:

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

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

Factores:

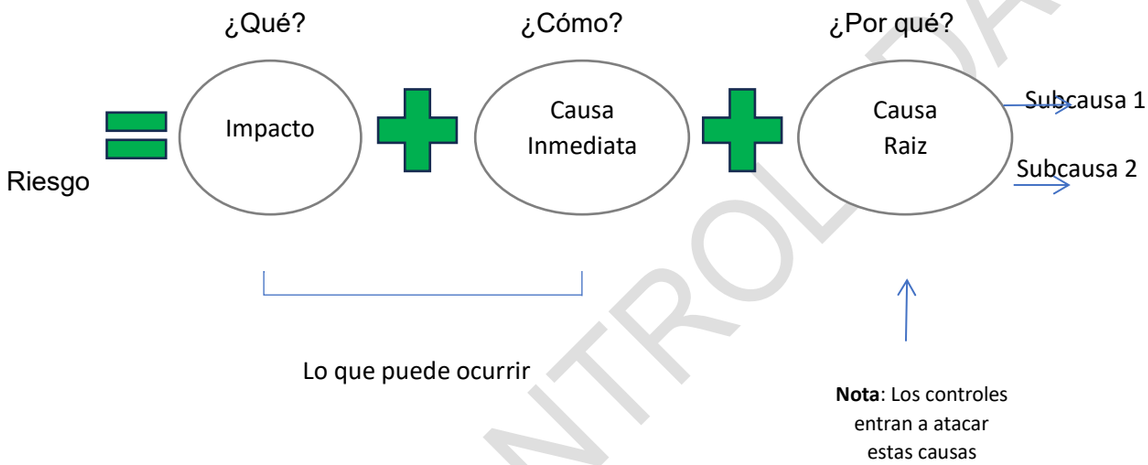
- Recursos públicos mal utilizados
- Desvío de presupuesto
- Pérdidas por actos de corrupción

Se deben identificar las fuentes generadoras del riesgo, es decir, las causas del riesgo, para ello se deben utilizar preguntas de referencia: ¿cómo puede suceder?, ¿por qué puede suceder? y, posteriormente identificar ¿qué consecuencias tendría su materialización?

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurtos activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura			Derrumbes

	Eventos relacionados con la infraestructura física de la entidad.		
			Incendios
			Inundaciones
			Daños a activos fijos

Asimismo, se debe incluir la descripción del riesgo que contenga todos los detalles necesarios para que se pueda entender, y para ello se deben tener en cuenta las siguientes frases: lo que puede ocurrir (qué), cuál es la causa inmediata (cómo) y finalmente la causa raíz (¿por qué?). Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2020.

La totalidad de riesgos que se identifiquen en el mapa de riesgos de cada proceso estarán sujetos al monitoreo, ajuste, control y seguimiento por parte de los líderes y su equipo de trabajo; lo cual incluye acciones que permitan combatir el riesgo para Reducirlo, Aceptarlo o Evitarlo y ser tratados al interior de cada proceso de acuerdo con la severidad del riesgo para Transferir o Mitigarlo.

En el caso de los riesgos de corrupción, estos no admiten aceptación del riesgo, por lo cual siempre deben tener un tratamiento con acciones precisas.

De acuerdo con lo establecido en la mencionada Guía de Administración del Riesgo del DAFP, versión 6, los riesgos se clasifican en las siguientes categorías:

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares. comisión de hechos delictivos abuso de confianza, apropiación indebida. incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para si mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones. interrupción de servicios básicos

Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo. salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Adaptado del Corso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2020

8.1 CLASIFICACIÓN DE RIESGOS

Riesgos Estratégico: es la posibilidad de que ocurran eventos o decisiones que afecten el cumplimiento de los objetivos misionales.

Riesgos Operativo: es la probabilidad de incurrir en pérdidas, retrasos o incumplimientos institucionales. Se origina por fallas en procesos internos, errores humanos, sistemas tecnológicos inadecuados o eventos externos que afectan el funcionamiento normal de una entidad.

Riesgo Fiscal: es la probabilidad de que ocurra un evento que cause daño, pérdida o detrimento al patrimonio y recursos del Estado.

Riesgo de Corrupción: es la probabilidad de que ocurra un evento que cause daño, pérdida o detrimento al patrimonio y recursos del Estado.

Riesgo de Seguridad de la Información: es la probabilidad de que se vulnere la confidencialidad, integridad o disponibilidad de los datos estatales.

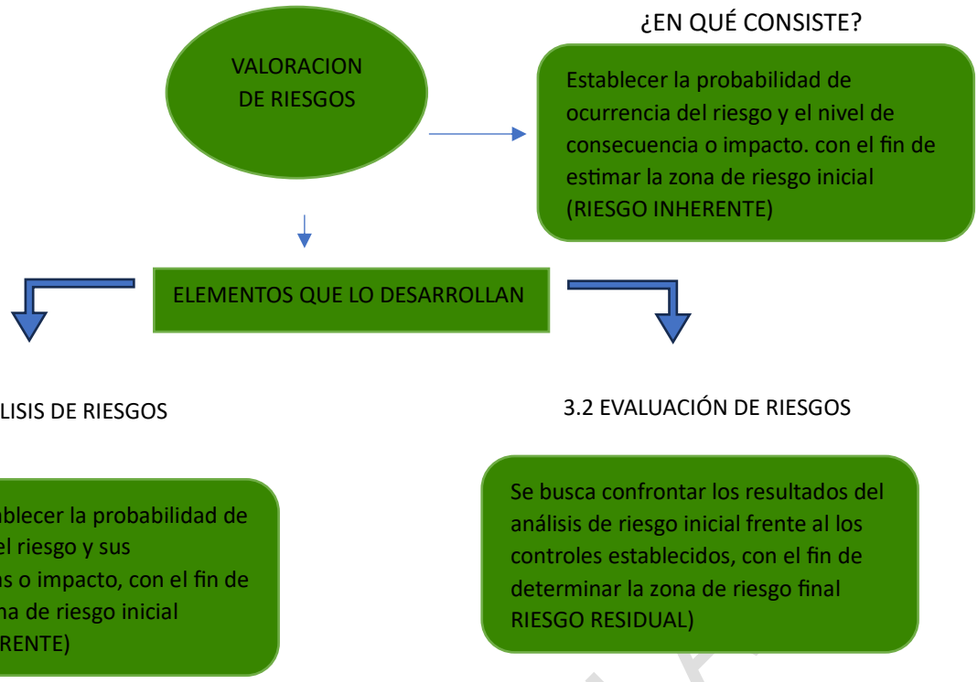
Riesgo SST: Consiste en identificar, evaluar y controlar los peligros que puedan afectar a los servidores públicos mediante la implementación obligatoria del SG-SST - Decreto 1072 de 2015 – Decreto Único Reglamentario en el Sector Trabajo y Resolución 032 del 2019 Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo.

Riesgo Legal: es la posibilidad de sufrir sanciones disciplinarias, fiscales o penales, así como daños patrimoniales, derivados del incumplimiento de leyes, normativas, contratos o políticas internas durante el ejercicio de las funciones.

Riesgo Financiero: es la probabilidad de sufrir pérdidas o daños en el patrimonio del Estado debido a una mala ejecución presupuestal, errores en los estados financieros, o un manejo inadecuado de tesorería y bienes.

9. VALORACIÓN DE RIESGOS

La valoración del riesgo en el IMEBU busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública 2018

9.1 Análisis del Riesgo

El análisis del riesgo dependerá de la información obtenida en el formato de identificación de riesgos y de la disponibilidad de datos históricos y aportes de los servidores de la entidad.

9.1.1 Criterios para definir el nivel de probabilidad

Para realizar la valoración de los riesgos, se califica la probabilidad de ocurrencia del riesgo y el impacto con las siguientes tablas:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 12 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 13 a 120 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 121 veces al año y máximo 1000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 1000 veces por año	100%

9.1.2 Determinar el impacto de los Riesgos de Proceso

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

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

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

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

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 12 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 13 a 120 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 121 veces al año y máximo 1000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 1000 veces por año	100%

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

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2020.

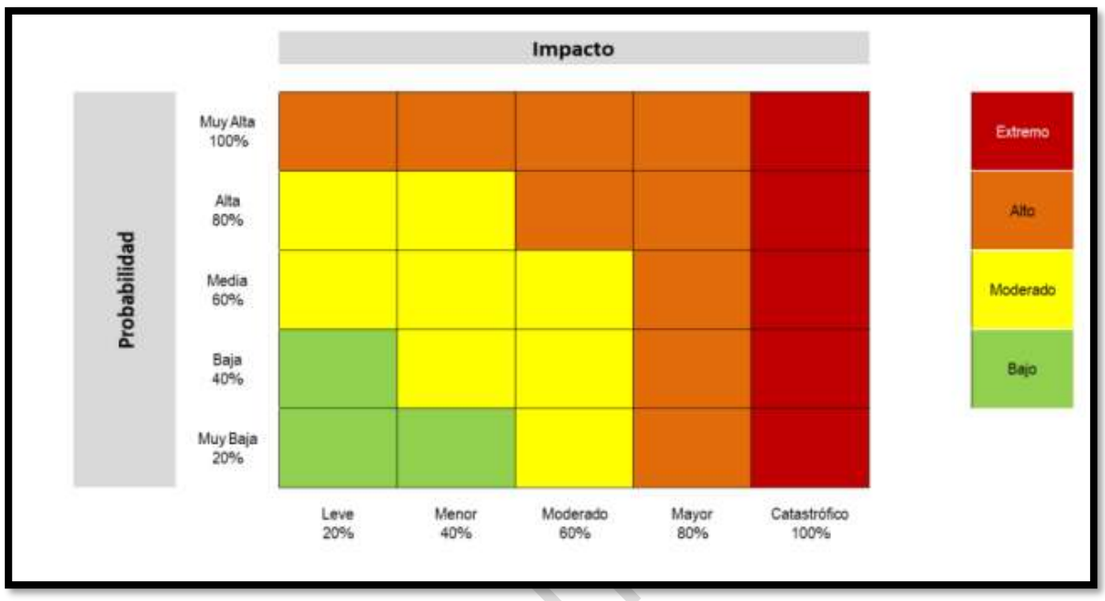
La afectación económica se calcula en 500 SMLMV, el impacto del riesgo es mayor.

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

9.2 Evaluación del Riesgo

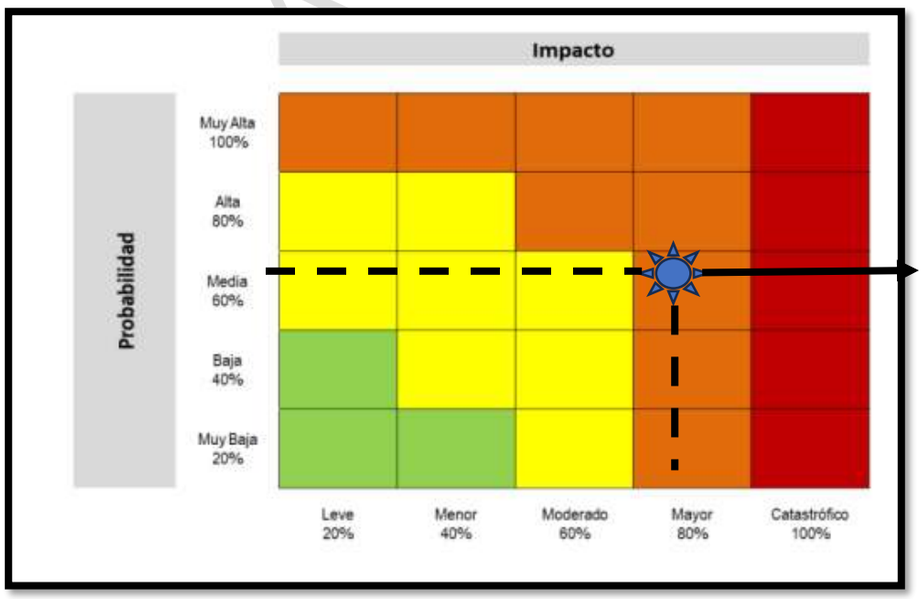
A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Análisis preliminar (riesgo inherente): Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020

Continuando con el ejemplo donde la Probabilidad inherente = media 60%, y el Impacto inherente: mayor 80%, se aplica la Matriz de Calor (Matriz identificación del Riesgo):



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

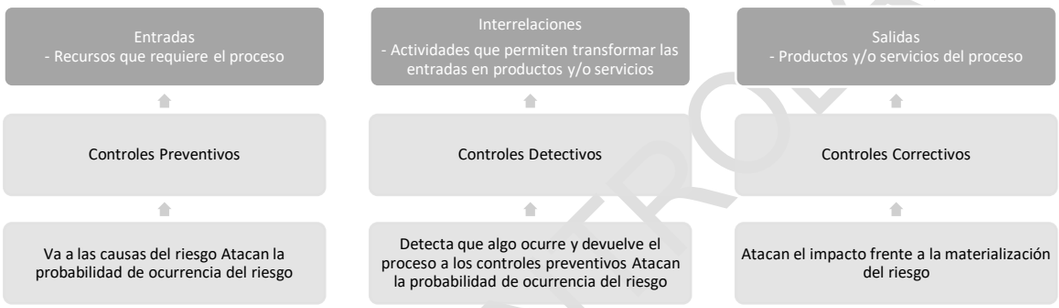
Valoración de controles: un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración.

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

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño institucional de Función Pública, 2020.

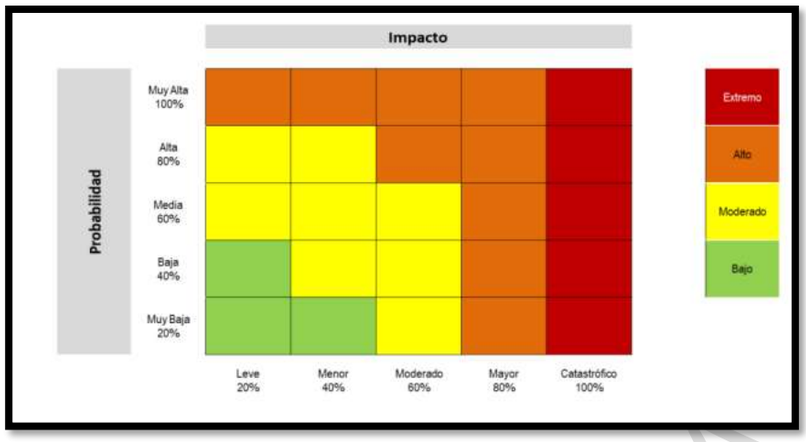
Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

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

Controles Correctivos → Atacan Impacto

Preventivos y Detectivos → Atacan probabilidad



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño institucional de Función Pública. 2020.

9.3 Estrategias para combatir el riesgo

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

Reducir

Implementar controles para reducir la probabilidad o el impacto.

Compartir

Compartir las consecuencias de la materialización del riesgo, por

ejemplo, a través de la adquisición de una ciber póliza

Plan de Acción

Evitar

Cuando se decide eliminar el activo que es fuente del riesgo: por ejemplo,

dar de baja un servidor

Aceptar

Cuando el nivel del riesgo está por debajo del apetito establecido por la

alta dirección.

Para todos los casos en que subsista un riesgo residual, se debe definir un plan de manejo del riesgo. Así, mientras el control hace referencia actividades rutinarias que se ejecutan en el desarrollo de la prestación de un servicio o la ejecución de una actividad, para evitar la materialización del riesgo (inherente), el plan de manejo hace referencia a actividades adicionales no rutinarias que ayudan a evitar la materialización del riesgo residual, y que requieren un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Ejemplo:

Riesgo	zonRInh	Control	Zon R. Resid	Plan Acción	Responsable	Fecha implementación	Fecha Seguimiento	Seguimiento	Estado
Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos.	Zona alta	Control 1 El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación. Control 2 El jefe de del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.	Zona alta	Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantad las actividades de levantamiento de requerimientos funcional es para la automatización de la lista de chequeo.	En curso

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, DAFP - diciembre de 2020, construido con base al ejemplo págs. 52 a 56

10. SEGUIMIENTO A LOS MAPAS DE RIESGOS Y CONTROLES

10.1). Los riesgos deberán actualizarse y validarse de manera permanente, considerando las condiciones de operación internas y externas que puedan afectar el cumplimiento de los objetivos institucionales, sin estar sujetos a una vigencia específica.

10.2) Cada líder de proceso será responsable de actualizar el análisis de contexto, riesgos y controles como resultado de los ejercicios de autocontrol, autoevaluación, evaluación independiente o por decisión del Comité Institucional de Coordinación de Control Interno (CICCI), cuando se considere necesario para garantizar el cumplimiento de los objetivos del proceso.

10.3) La revisión y actualización integral de los riesgos se realizará, por lo menos una vez al año, con el acompañamiento del Profesional de Apoyo de MIPG Institucional y la asesoría de la Oficina de Control Interno.

10.4) El Programa de Transparencia y Ética Pública (PTEP), se publicará a más tardar el 31 de enero de cada año de acuerdo con el nivel del riesgo residual, la periodicidad para el seguimiento del riesgo se determina de acuerdo con los niveles de aceptación del riesgo.

10.5) Cada proceso reportará trimestralmente a la segunda línea de defensa a través del Mapa de Riesgos de Gestión de Institucional, el estado de la Gestión de las acciones y controles formulados junto con las evidencias correspondientes, describiendo concretamente si hubo o no riesgos materializados.

10.6) Si se identifican riesgos materializados por cualquiera de las líneas de defensa, de manera inmediata se ejecutan las acciones de contingencia para su tratamiento, previa realización del análisis de causas correspondiente.

10.7) Se establece que la oficina de Control Interno realiza los seguimientos a la Política de Administración del Riesgo en las fechas establecidas en sus cronogramas y cuando se requiera.

10.8) Los entregables se realizarán cuatro veces al año de la siguiente manera:

	Fecha Límite Entregable
Trimestre I	10 de abril
Trimestre II	10 de julio
Trimestre III	10 de septiembre
Trimestre IV **Entrega Parcial** **Entrega Final**	*1 - 10 de diciembre *2 - 10 de enero

*1 Nota: Entregable parcial octubre, noviembre y 10 de diciembre.

*2 Nota: Entregable final diciembre 11 al 30. El personal de planta será el encargado de recolectar las evidencias de los días 11 al 30 de diciembre, posteriormente el Profesional de Apoyo de MIPG Institucional realizará el monitoreo y entregará a la oficina de Control Interno a los veinte (20) días del mes de enero para el respectivo seguimiento.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Programa de Transparencia y Ética Pública (PTEP) en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

La frecuencia de seguimiento a los riesgos residuales y sus respectivos controles se indica en la siguiente tabla, según el tipo de riesgo:

RIESGO DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN	
ZONA DE RIESGO RESIDUAL	**ESTRATEGIA DE SEGUIMIENTO**
Bajo	Se realiza seguimiento trimestral y se registran sus avances en la herramienta tecnológica dispuesta para tal fin.
Moderado	Se realiza seguimiento trimestral y se registran sus avances en la herramienta tecnológica dispuesta para tal fin.
Alto	Se realiza seguimiento trimestral y se registran sus avances en la herramienta tecnológica dispuesta para tal fin.
Extremo	Se realiza seguimiento trimestral y se registran sus avances en la herramienta tecnológica dispuesta para tal fin.

RIESGO DE CORRUPCIÓN	
ZONA DE RIESGO RESIDUAL	**ESTRATEGIA DE SEGUIMIENTO**
Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran deben tener un seguimiento semestral tal como lo indica el Programa de Transparencia y ética Pública y se registrará en el módulo de riesgos en la herramienta tecnológica dispuesta para tal fin, sin embargo, en la entidad se realizará el seguimiento trimestralmente.	

11. MECANISMOS DE COMUNICACIÓN DE LA POLÍTICA Y RESULTADOS DE LA ADMINISTRACIÓN DE RIESGOS

La política para la administración de riesgos busca crear conciencia en todos los servidores públicos del Instituto Municipal de Empleo y Fomento Empresarial de Bucaramanga, independiente del nivel de cargo y el tipo de vinculación, sobre la importancia de la gestión preventiva y el autocontrol en la ejecución de las actividades. En ese sentido, se adelantarán acciones o estrategias de comunicación y divulgación de la política y sus resultados según su propósito:

- ✓ A nivel institucional: La divulgación y socialización de la Política de Administración del Riesgo y la Matriz de Riesgos, la cual estará a cargo del Profesional de Apoyo de MIPG Institucional y del director del instituto, esta estrategia incluye la publicación en la página web de la Entidad y los canales internos, (Programa de Transparencia y Ética Pública).
- ✓ A nivel de procesos: La divulgación de la matriz de riesgos por proceso al interior de los respectivos equipos de trabajo, la cual está a cargo de los lideres de cada proceso, y el Profesional de Apoyo de MIPG Institucional estará disponible para brindar apoyo.
  Se hace entrega de los respectivos informes: Entendiendo que la etapa de comunicación y consulta tiene como objetivo el intercambio de información y la presentación de resultados ante las instancias correspondientes para la toma de decisiones, es una parte fundamental de esta la difusión de los informes ante la alta dirección, los procesos y dependencias de la entidad y los entes de control tanto interno como externos. Lo anterior, con el fin que los informes sean difundidos oportunamente y sirvan como insumo para la toma de decisiones a nivel estratégico, operative o ambos.

- ✓ La gestión de la política de administración del riesgo al interior del Instituto se orienta al cumplimiento de resultados medibles, estos resultados se obtienen a partir del proceso de evaluación y seguimiento de la política, el cual se apoya en la aplicación de la matriz de riesgos como herramienta principal para identificar, valorar y controlar los riesgos institucionales.
- ✓ En el marco de la Política de Administración del Riesgo en la Función Pública, la entidad debe orientar su gestión al cumplimiento de resultados verificables. Para ello, cuenta con un tablero de control general que forma parte del mapa de riesgos de gestión institucional y permite realizar el seguimiento y monitoreo de los riesgos identificados en el interior del Instituto.