

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 1 de 39	

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 2 de 39	

Contenido

1.	Introducción	4
2.	Objetivo	5
3.	Alcance	5
4.	Aspectos positivos de la gestión de Riesgos	5
5.	Niveles de aceptación del riesgo o tolerancia al riesgo.....	6
6.	Términos y definiciones	6
7.	Estructura para la gestión del riesgo	8
7.1	Metodología a utilizar	9
8.	Etapas de la administración de riesgos.....	9
8.	Lineamientos	11
8.1.	Lineamientos operativos para Mapas de Riesgos institucionales, Corrupción y seguridad de la información	12
8.2.	Comunicación y Socialización de la Política de Gestión del Riesgo	13
8.3.	Monitoreos.....	13
8.4.	Directrices para la conservación de evidencia.....	13
8.5.	Seguimiento.....	14
9.	Roles y Responsabilidades	14
10.	Metodología para el tratamiento de riesgos.....	18
10.1.	Tratamiento Riesgos de Gestión y Fiscales	18
10.1.1.	Zona de riesgo y tratamiento	18
10.1.2.	Probabilidad	19
10.1.3.	Impacto	20
10.1.4.	Mapa de calor.....	20
10.1.5.	Valoración de controles	21
10.1.6.	Análisis y evaluación de los controles	21
10.1.7.	Nivel de Riesgo (Riesgo Residual)	22
10.1.8.	Manejo de riesgos	22
10.1.9.	Directrices para la redacción de riesgo Fiscal	23
10.2.	Tratamiento Riesgos de Corrupción	24
10.2.1.	Zona de riesgo y tratamiento	26
10.2.2.	Directrices de redacción para riesgos de corrupción	27

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 3 de 39	

10.3. Tratamiento de Riesgos de Seguridad y Salud en el Trabajo	28
10.3.1 Identificación de Peligros y Valoración de los Riesgos.....	28
10.3.2 Aspectos para tener en cuenta al desarrollar la identificación de los peligros y la valoración de los riesgos.....	29
10.3.3 Actividades para identificar los Peligros y Valorar los Riesgos.....	30
10.3.4 Descripción y clasificación de los peligros.....	33
10.4 Tratamiento Riesgos de seguridad Digital.....	34
10.4.1 Planes de tratamiento de Riesgos de Seguridad Digital e indicadores para la gestión del Riesgo.....	34
10.4.2 Fase 2. Ejecución.....	34
10.4.3 Fase 3. Monitoreo y Revisión.....	35
10.4.4 Reporte de la gestión del riesgo de Seguridad digital al interior de la entidad pública	35
10.4.5 Auditorías internas y externas.....	36
10.4.6 Medición del Desempeño.....	36
10.4.7 Mejoramiento continuo de la gestión del riesgo de Seguridad Digital.....	36
11. Riesgos de Seguridad y Salud en el trabajo	37
12. Riesgos Ambientales	37
13. Comunicación y consulta	37
14. Control de cambio	38
15. Ruta de Aprobación.....	39

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 4 de 39	

1. Introducción

La administración del Riesgo comprende el conjunto de Elementos de Control y sus Interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales; contribuye a que la entidad consolide su Sistema de Control Interno y a generar una cultura de Autocontrol y autoevaluación al interior de la misma.

Teniendo en cuenta que la administración de riesgos es estratégica para el logro de los objetivos institucionales y de procesos, en este manual se enuncia la política marco de acción que permitirá tomar decisiones relativas a la administración del riesgo, el cual está alineado y armonizado con el Modelo Integrado de Planeación y Gestión MIPG, la Guía para la Gestión del Riesgo establecida por el Departamento Administrativo de la Función Pública, el manual para la identificación y cobertura del riesgo en los procesos de contratación y la Norma Técnica sobre Gestión del Riesgo, ISO 31001.

La tendencia más común es la valoración del riesgo como una amenaza; en este sentido, los esfuerzos institucionales se dirigen a reducir, mitigar o eliminar su ocurrencia. No obstante, el riesgo como oportunidad, implica que su gestión está dirigida a optimizar los resultados que este genera.

En tal sentido, la **Alcaldía Municipal de Ibagué**, no es inmune al riesgo, es más, los riesgos de la Entidad cambian constantemente y la naturaleza y las consecuencias potenciales que se enfrentan son cada vez más complejas y sustanciales. La rapidez del cambio, la creciente complejidad de la economía mundial, las expectativas más exigentes de la comunidad, los requerimientos del estado colombiano, el impacto de una posible falla en los controles, los rápidos cambios en las tecnologías y un sinnúmero de otros factores pueden afectar la Entidad, de manera tal que se requiere de una alta y oportuna capacidad, así como de una estructura organizacional preparada.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 5 de 39	

2. Objetivo

Definir la metodología y lineamientos de la política integral de gestión del riesgo, a través de la identificación de acciones de control, respuestas oportunas y estrategias institucionales, con el propósito de atacar las causas potenciales, las amenazas, las vulnerabilidades y minimizar los impactos ante una eventual materialización que puedan afectar la misionalidad, las estrategias y objetivos Institucionales.

3. Alcance

La política de administración de riesgos es aplicable a todos los procesos de la Entidad y a las acciones ejecutadas por los servidores y/o contratistas durante el ejercicio de sus funciones. Incluye los principios básicos y metodológicos para la administración y gestión de riesgos y oportunidades de tipo estratégico, operacional y de cumplimiento.

En el caso de los riesgos de seguridad digital debe ser extensible y aplicable a los procesos de la entidad que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información, habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

4. Aspectos positivos de la gestión de Riesgos

- **Alinea el riesgo y la estrategia:** cuando en la prospectiva institucional, la dirección considera los riesgos estableciendo puede orientar mejor los esfuerzos y los recursos para el logro de los objetivos, desarrollando mecanismos para gestionar las oportunidades o amenazas asociadas.
- **Mejora las decisiones de respuesta a los riesgos:** La gestión de riesgos proporciona rigor para identificar las posibles oportunidades o amenazas que hacen parte del quehacer institucional y seleccionar entre las posibles alternativas de respuesta la más viable y efectiva, para alcanzar los resultados esperados.
- **Reduce las sorpresas y las pérdidas operativas:** La gestión de los riesgos permite mejorar la capacidad de la entidad para identificar las amenazas o vulnerabilidades que pueden afectar su gestión y establecer respuestas, reduciendo la incertidumbre frente a eventos potenciales.
- **Identifica y gestiona la diversidad de riesgos para toda la entidad:** la gestión de riesgos desde un enfoque sistémico facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos, optimizar los recursos disponibles y garantizar la coherencia en las respuestas institucionales, en el momento de abordar las

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 6 de 39	

posibles vulnerabilidades o amenazas, así como las oportunidades identificadas.

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

5. Niveles de aceptación del riesgo o tolerancia al riesgo

Ningún riesgo de corrupción podrá ser aceptado

Los demás riesgos de gestión y los de seguridad digital identificados en zona de riesgo baja se aceptarán, y se administrarán por medio de las actividades propias de los procesos o procedimientos asociados.

6. Términos y definiciones

Administración de riesgos: Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino con la apropiación de la evaluación de los riesgos como una parte natural del proceso de planeación institucional. (INTOSAI, 2000).

Análisis de riesgo: Uso sistemático de la información disponible para valorar los riesgos en función de las causas o agentes que los generan, las consecuencias generadas por un incidente y/o evento, su severidad y la posibilidad de ocurrencia del mismo, con el fin de estimar la zona de riesgo inicial (riesgo inherente).

Apetito al Riesgo: Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

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.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 7 de 39	

impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación del riesgo: Determinación de las prioridades de gestión del riesgo, mediante la comparación del nivel de riesgo hallado (riesgo inherente) y la evaluación de las medidas de control existentes. Es una etapa que busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Fraude: Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapas de riesgo: Documento con la información resultante de la identificación, valoración y tratamiento del riesgo.

Monitoreo: Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo puede ser Probabilidad por Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

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

Plan de tratamiento de riesgos: Se define como las decisiones de tratamiento de los riesgos y las actividades de control para su mitigación, a través de la aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de ocurrencia de los riesgos, sus consecuencias o ambas.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 8 de 39	

Política de Administración del Riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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

Riesgo de fraude: Efecto que se causa sobre los objetivos de las Entidades, debido a una acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo Fiscal: Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, 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.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 9 de 39	

7. Estructura para la gestión del riesgo

7.1 Metodología a utilizar

Se utilizará para riesgos de Gestión la metodología vigente publicada por el Departamento Administrativo de la Función Pública DAFP para la administración del riesgo y el diseño de controles en entidades públicas versión 6 y/o la que modifique o sustituya. Para riesgos de corrupción la metodología adoptada es la establecida por la Secretaría de Transparencia de la Presidencia de la República.

Se utilizará la metodología vigente por Colombia Compra Eficiente, para la administración de riesgos para el proceso de contratación dirigido a los partícipes del sistema de compras y contratación pública.

Así como también se utilizará la metodología establecida por la guía técnica colombiana GTC 45 para la identificación de riesgos y peligros de Seguridad y Salud en el Trabajo, de igual manera se dará uso de la Guía técnica Colombiana GTC 104 para la identificación de riesgos ambientales. Para los riesgos de la seguridad digital, se aplican los lineamientos establecidos en el modelo de seguridad y privacidad de la información (MSPI) e interacción del Modelo Nacional de Gestión de Riesgos de seguridad Digital (MGRSD). El MSPI integra en cada una de sus fases asociadas a la gestión de riesgos de seguridad digital, ya que esta practica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el presente Anexo, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad digital requeridas en el MSPI.

8. Etapas de la administración de riesgos

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad. Con el fin de asegurar dicho manejo, en la Alcaldía Municipal de Ibagué, se adoptaron de la guía de administración del riesgo y el diseño de controles en entidades públicas las siguientes etapas (Ver Ilustración 1. Metodología para la administración del riesgo).

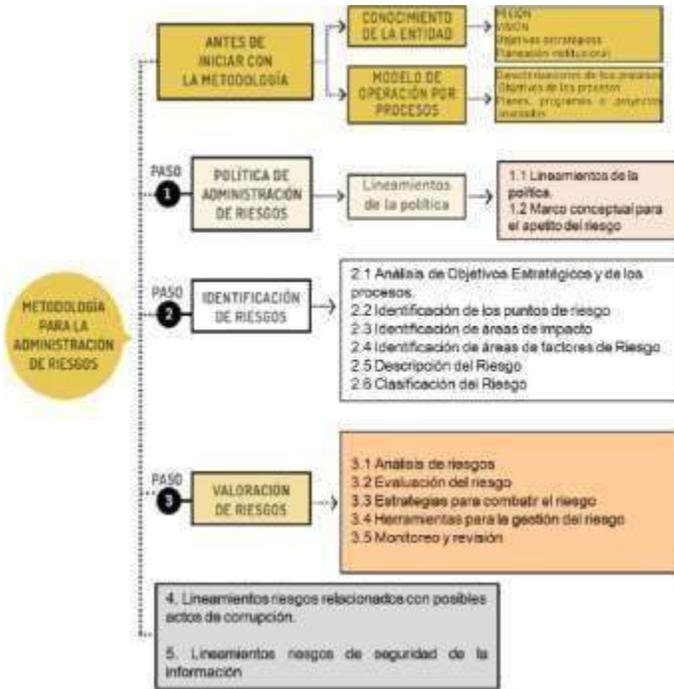


Ilustración 1. Metodología para la administración de riesgos de Gestión
 Tomado de: guía de administración del riesgo y el diseño de controles en entidades públicas

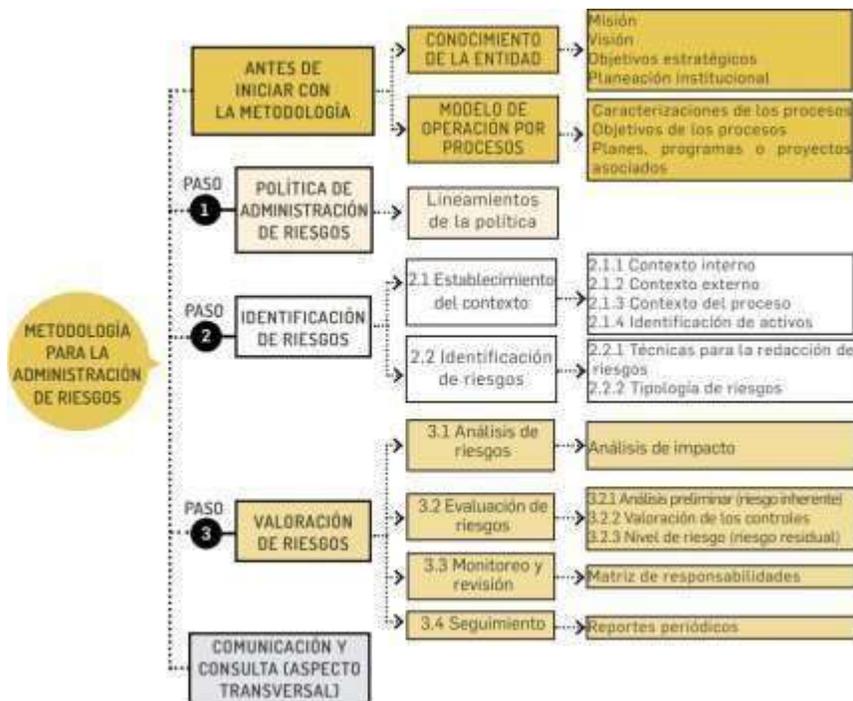


Ilustración 2 Metodología para la administración de riesgos de Corrupción
 Tomado de: guía de administración del riesgo y el diseño de controles en entidades públicas

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		POLITICA DE ADMINISTRACIÓN DEL RIESGO	
		Fecha: 03/12/2024	
		Página: 11 de 39	

8. Lineamientos:

El aspecto central para el desarrollo y la consolidación de la política de administración de riesgos, es la identificación y análisis del mapa de riesgos institucional y la formulación y actualización de la matriz de riesgos (matriz de calor y zonas de riesgo) con base en los siguientes criterios:

- Los riesgos siempre deben asociarse a los objetivos o estrategias definidas en la **Alcaldía Municipal de Ibagué**, objetivos de los procesos o proyectos. Un pre-requisito indispensable para trabajar en la identificación de riesgos consiste en el entendimiento uniforme y completo de los objetivos y estrategias que se establezcan en la Entidad, en el marco de su contexto estratégico.
- Los mapas de riesgos de gestión y corrupción serán de conocimiento de la alta dirección, y su riesgo residual será el soporte para aprobación y/o modificación de la política de administración del riesgo.
- Los mapas de riesgos deben estar alineados con el Sistema Integrado de Gestión y con la planeación estratégica de la entidad.
- Se deben focalizar los riesgos estratégicos y operacionales residuales que queden ubicados en zona de riesgos extremos y altos con propósito de toma de decisiones en cuanto a su tratamiento.
- La opción de tratamiento o manejo para los riesgos residuales ubicados en zona de riesgo moderado, alto o extremos, no se podrán aceptar según lo establece la metodología, esto considerando los eventos registrados para dichos riesgos en periodos anteriores, y a partir de este análisis deberán tener una propuesta o acción de tratamiento coherente que busquen gestionar el riesgo. *Nota: Aplica para riesgos de Gestión.*
- Los riesgos residuales que queden ubicados en zona de riesgo baja o muy baja podrán llevar cualquiera de las opciones de manejo indicadas por el presente manual “aceptar, evitar, reducir”. Si se elige como tratamiento para el riesgo la opción de “aceptar el riesgo”, significará que para la vigencia no se generarán nuevos planes de acción para mitigar el riesgo. Sin embargo, el que se incluya esta opción no excluye al líder de proceso de la obligación de continuar aplicando los controles establecidos, y hacer el respectivo seguimiento tanto a los controles ya implementados como a la posible materialización del riesgo. Para riesgos de corrupción y/o soborno no se puede aceptar o asumir el riesgo.
- Se mantiene el protocolo para la identificación de riesgos de corrupción, asociados a la prestación de trámites y servicios, en el marco de la política de racionalización de trámites, liderado por la dirección de participación, transparencia y servicio al ciudadano de Función Pública.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 12 de 39	

- Para los riesgos de seguridad digital se debe implementar el anexo 4 'Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas' de la Guía para la administración de riesgos y el diseño de controles en entidades públicas, bajo el lineamiento del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).

8.1. Lineamientos operativos para Mapas de Riesgos institucionales, fiscales, corrupción y seguridad de la información.

- Los mapas de riesgos deberán ser aprobados por los líderes de los correspondientes procesos. Sin embargo, La Dirección de Fortalecimiento Institucional, la Oficina de Control Interno y/o el Comité Institucional de Gestión y Desempeño, podrán solicitar se incluyan en el Mapa de Riesgos, aquellos riesgos potenciales que no hayan sido incluidos en los mapas de riesgos por procesos.
- Para los riesgos de la norma antisoborno ISO37001, Corresponde a los riesgos de corrupción establecidos por el departamento administrativo de la función pública.
- Los mapas de riesgos deberán ser consolidados, publicados y socializados.
- Los mapas de riesgo deben como mínimo cubrir los riesgos asociados a las políticas MIPG (Gestión presupuestal y eficiencia del gasto público, talento humano, integridad, fortalecimiento organizacional y simplificación de procesos, servicio al ciudadano, participación ciudadana en la gestión pública, racionalización de trámites, gestión documental, gobierno Digital).
- La actualización de los mapas institucionales de riesgos de gestión, así como los mapas de riesgos de corrupción y seguridad digital de demás modelos referenciales se realizarán de forma anual según lineamientos normativos, salvo que las necesidades del servicio requieran su actualización con otra periodicidad.
- La eliminación de cualquier riesgo deberá ser debidamente justificada y aprobada por el líder del proceso y deberá registrarse en la matriz de cambios (eventos) de la Entidad.
- Teniendo en cuenta la norma ISO 27001 de Seguridad de la Información, la secretaria de TIC** deberá actualizar los riesgos de seguridad de la información a los que se puedan ver expuestos los diferentes procesos de la Entidad, teniendo en cuenta los principios de gestión de riesgos para procesos de la presente guía.
- Los riesgos de seguridad digital por su naturaleza e impacto se clasificarán como información pública clasificada, cuya publicación será parcial fundamentada en el índice de clasificación de la información en la que se deberá anonimizar la información clasificada y reservada, así como las vulnerabilidades y controles, a fin de evitar su exposición, lo cual podría facilitar ataques cibernéticos y uso indebido de la información de terceros.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 13 de 39	

8.2. Comunicación y Socialización de la Política de Gestión del Riesgo

La política de administración del riesgo en el Municipio de Ibagué será comunicada a todos los niveles de la organización, mediante alguno de los siguientes canales:

- Página WEB de la Entidad
- Correos electrónicos
- Procesos de Formación y Capacitación
- Ejercicios de Inducción y Re-Inducción

A través de estos canales se comunica o socializa contenidos relacionados con la gestión de los riesgos y aquellos orientados a generar conocimiento en los funcionarios y contratistas de la entidad.

8.3. Monitoreos.

Los monitoreos les corresponden a la línea estratégica, primera y segunda línea de defensa. Se desarrollarán de la siguiente manera:

Línea Estratégica: En comité de coordinación de control interno realizará seguimiento a la política y a la gestión de los riesgos según la programación de los comités de control interno establecidos en el plan anual de auditoría.

Primera Línea de Defensa: Realiza monitoreo bimestral a las acciones tendientes a controlar y gestionar los riesgos y enviará a la Secretaría de Planeación los resultados de esos monitoreos cinco días antes de terminarse el bimestre.

La primera línea de defensa realizará reporte bimestralmente o cuando ocurra la materialización de riesgos materializados en la matriz de gestión de eventos

Segunda Línea de Defensa: Realizará monitoreo bimestral a través de los informes que los líderes de procesos remitan, asegurando que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

8.4. Directrices para la conservación de evidencia.

Es responsabilidad de los líderes de los procesos y sus equipos de trabajo conservar la evidencia de la aplicación de los controles formulados para prevención de la materialización de los riesgos, durante por lo menos cinco (5) años posteriores a la ejecución de los controles y garantizar la disponibilidad de la evidencia a los entes de control si se diera el caso.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 14 de 39	

8.5 Seguimiento

Tercera línea de defensa, la oficina de control interno. Quien provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La periodicidad de la evaluación de los riesgos por parte de la Oficina de Control Interno, se definirá de acuerdo con los lineamientos generados por la secretaria de Transparencia de la Presidencia de la Republica y por el Departamento Administrativo de la Función Pública para los riesgos de corrupción y para para los riesgos de gestión serán la periodicidad por la Oficina de Control Interno.

Si algún riesgo se llegara a materializar y esto es detectado por el líder del proceso se debe seguir los siguientes pasos:

1. Informar o reportar al Representante de la Alta Dirección para el MIPG.
2. De ser necesario, realizar la denuncia ante el ente de control respectivo
3. Iniciar las acciones correctivas necesarias.
4. Realizar el análisis de causas y determinar acciones de mejora.
5. Actualizar el mapa de riesgos.
6. Diligenciar el formato de Matriz de gestión de eventos y remitir a la dirección de fortalecimiento institucional

Además de la evaluación de riesgos, la Oficina de Control Interno valorará el diseño del control y la efectividad de los controles para prevenir la materialización de los riesgos.

Si la oficina de Control Interno en los seguimientos establecidos evidencia que un riesgo de corrupción se materializó, debe seguir los siguientes pasos:

1. Comunicar a la alta dirección en Comité de Coordinación de Control Interno e informar sobre los hechos detectados, a las respectivas dependencias para que tomen las medidas correctivas según corresponda
2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.
3. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos

9. Roles y Responsabilidades

Los Roles y Responsabilidades para la Administración del Riesgo por Procesos, definidos en la Entidad, son las siguientes:

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 15 de 39	

Línea de Defensa	Responsable	Responsabilidad Frente al Riesgo
Línea Estratégica	<ul style="list-style-type: none"> - ALTA DIRECCIÓN - Comité de Coordinación de Control Interno 	<p>Esta línea al ser una instancia decisoria dentro del sistema de Control Interno, su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes dela entidad. Así mismo debe revisar, validar y supervisar el cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la Línea Estratégica son:</p>
		<ul style="list-style-type: none"> - Fortalecimiento del Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para lasreuniones. - Evaluación de la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica. - Definición de líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. - Definición y evaluación de la Política de Administración delRiesgo. La evaluación debe considerar su aplicación en laentidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. - Evaluación de la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar) - Define el marco general para la gestión del riesgo y el control; y supervisa su cumplimiento.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG		Código: POL-SIG-01	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO		Versión: 11	
			Fecha: 03/12/2024	
			Página: 16 de 39	
Primera Línea de Defensa	<ul style="list-style-type: none"> - Líderes de Procesos. (GERENTES PÚBLICOS) 	<p>Esta línea de defensa les corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad. Se debe precisar que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles de gerencia operativa, ya que son aplicados por líderes o responsables de proceso. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos. Los aspectos clave para el Sistema de Control Interno (SCI) a tener en cuenta por parte de la 1ª Línea:</p> <ul style="list-style-type: none"> - Está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos entodoslos niveles de la organización); su rol principal es el mantenimiento efectivo de controles internos, la ejecuciónde gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del“Autocontrol”. - El conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. - La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. - El seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. - La formulación de planes de mejoramiento, su aplicación yseguimiento para resolver los hallazgos presentados - La coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. 		
Segunda Línea de Defensa	<ul style="list-style-type: none"> - Los responsables se encuentran relacionados en el Mapa de Aseguramiento. En cumplimiento del lineamiento establecido en el Manual de MIPG: - Líderes de los procesos: Dirección de Fortalecimiento 	<ul style="list-style-type: none"> - Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. - Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impactode los riesgos. - Evaluar y efectuar seguimiento a los controles aplicados por la 1ª línea de defensa. 		

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 17 de 39	

		<ul style="list-style-type: none"> - Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. - Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. - Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. - Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio. - Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del Comité de Coordinación de Control Interno - Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad.
	Dirección de Planeación de Desarrollo	<ul style="list-style-type: none"> - Seguimiento Al cumplimiento de las metas del plan de desarrollo (Plan Indicativo). - Seguimiento al Plan Anual de Adquisiciones.
	Secretario(a) de las TIC	<ul style="list-style-type: none"> - Implementación y seguimiento al Plan estratégico de TIC (PETIC) y Seguimiento a la aplicación de las políticas de seguridad de la información. - Seguimiento al Sistema de Gestión de Seguridad de la información
	Secretario(a) Administrativa – Director(a) Recursos Físicos	<ul style="list-style-type: none"> - Seguimiento a la aplicación de las Tablas de Retención Documental.
	Jefe de Oficina Jurídica	<ul style="list-style-type: none"> - Seguimiento a las sentencias judiciales o fallos en contra del Municipio.
	Director(a) de Servicio y Atención al Ciudadano.	<ul style="list-style-type: none"> - Seguimiento a la oportunidad de respuesta de las PQRS al interior de los Procesos - Seguimiento al comportamiento de los reclamos al interior de los Procesos
	Director(a) de Talento Humano.	<ul style="list-style-type: none"> - Evaluación del Plan Estratégico de Talento Humano - Seguimiento al cumplimiento de los principios y valores establecidos en el código de integridad por parte de los servidores públicos - Seguimiento al cumplimiento a la declaraciones e identificación de posibles conflictos de intereses, establecidos en el código de integridad por parte de los servidores públicos
	Director(a) de Fortalecimiento Institucional	<ul style="list-style-type: none"> - Consolidación de Indicadores del Sistema Integrado de Gestión SIGAMI - Auditorías Internas - Seguimiento al cumplimiento de los requisitos de las Normas HSEQ - Realizar seguimiento a los indicadores de incidentes, accidentes de trabajo, enfermedades laborales y ausentismo por enfermedad común.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		POLITICA DE ADMINISTRACIÓN DEL RIESGO	

Tercera Línea de Defensa	– Oficina de Control Interno	<ul style="list-style-type: none"> – Esta línea está bajo la responsabilidad de la (el) Jefe de control interno; quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa (proveedores internos de aseguramiento) y la 3ª línea de defensa y estas con los proveedores externos de aseguramiento (organismos de control y otras instancias de supervisión o vigilancia), serán representadas en una matriz de doble entrada denominada mapa de aseguramiento, herramienta considerada por el Instituto de Auditores como adecuada e idónea para coordinar las diferentes actividades de aseguramiento, visualizar el esfuerzo en común y mitigar los riesgos de una manera más integral. – Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 3ª Línea: – A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimiento efectivo de los objetivos – Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. – Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. – Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. – Informar los hallazgos y proporcionar recomendaciones de forma independiente.
---------------------------------	-------------------------------------	---

10. Metodología para el tratamiento de riesgos

El tratamiento de riesgos es la respuesta establecida por la línea estratégica para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para los procesos, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo.

10.1. Tratamiento Riesgos de Gestión y Riesgos Fiscales.

10.1.1. Zona de riesgo y tratamiento:

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 19 de 39	

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de Gestión, fiscal	Muy baja o Baja	Se ACEPTA el riesgo y se administra por medio de las actividades propias del proceso o procedimiento asociado y se realiza en el reporte bimensual de sudesempeño.
y seguridad digital	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se hace monitoreo bimestral y se registran sus avances en la matriz establecida para tal fin.
	Alta y Extrema	Se adoptan medidas para REDUCIR O COMPARTIR la probabilidad o el impacto del riesgo, o ambos; esto conlleva a la implementación de controles. Periodicidad bimestral.

10.1.2. Probabilidad

Se entiende por probabilidad como la posibilidad de ocurrencia del riesgo. La probabilidad de ocurrencia estará asociada a la **exposición al riesgo** del proceso o actividad que se esté analizando.

De este modo, la probabilidad inherente será el **número de veces que se pasa por el punto de riesgo en el periodo de 1 año.**

Para su determinación se utiliza la tabla de probabilidad (ver Tabla 4 - Criterios para definir el nivel de probabilidad. Guía DAFP versión 6)

Tabla 1 Probabilidad

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

Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V6.

10.1.3. Impacto:

Se adopta la siguiente tabla con los criterios para calificar el Impacto – riesgos de gestión y riesgo fiscal.

Tabla 2 Impacto

Nivel	Impacto (consecuencias)	
	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 menor o igual a 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%	Mayor a 50 menor o igual 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 menor o igual 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: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6.

10.1.4. Mapa de calor

Para poder identificar la zona de riesgo y los niveles de severidad, se utilizará el siguiente mapa de calor a través de la combinación de la probabilidad y el impacto determinados tanto para los riesgos inherentes como para los residuales.

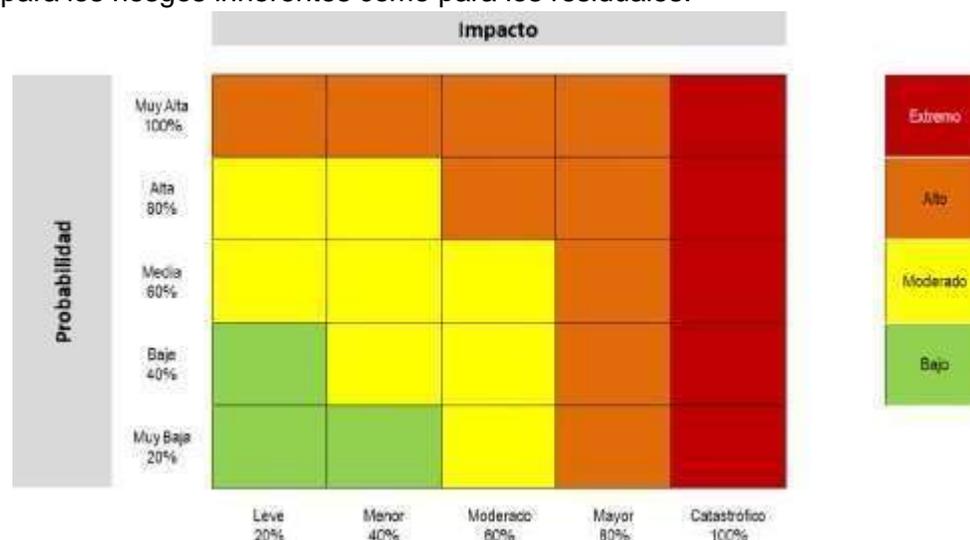


Ilustración 3 Mapa de calor

Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 21 de 39	

10.1.5. Valoración de controles

Un control se define como la medida que permite reducir o mitigar el riesgo.

Nota: La valoración de controles se ha establecido conforme la metodología establecida en la página 45 de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6.

10.1.6. Análisis y evaluación de los controles

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así.

Características		Descripción		
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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

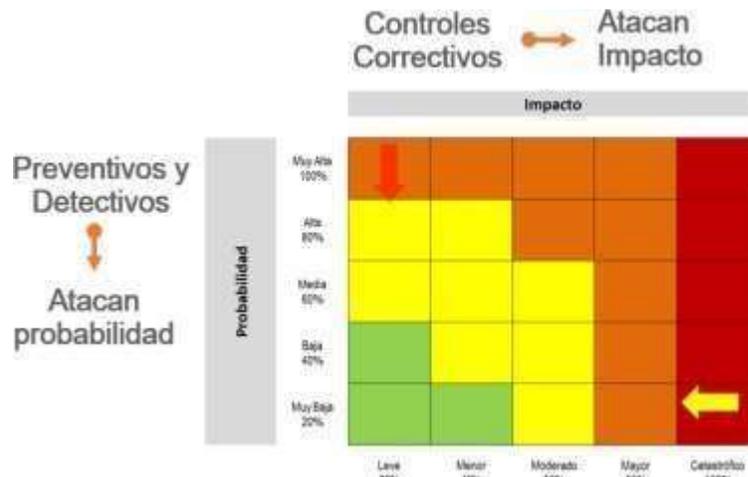


Ilustración 4 matriz de calor

Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6.

10.1.7. Nivel de Riesgo (Riesgo Residual).

El riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control (*Ver. Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6. Apartado 3.2.3.*).

10.1.8. Manejo de riesgos

Opción para el manejo del riesgo	Descripción
Evitar el riesgo	<p>Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.</p> <p>Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.</p>
Compartir el riesgo	<p>Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.</p> <p>Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.</p> <p>Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.</p>

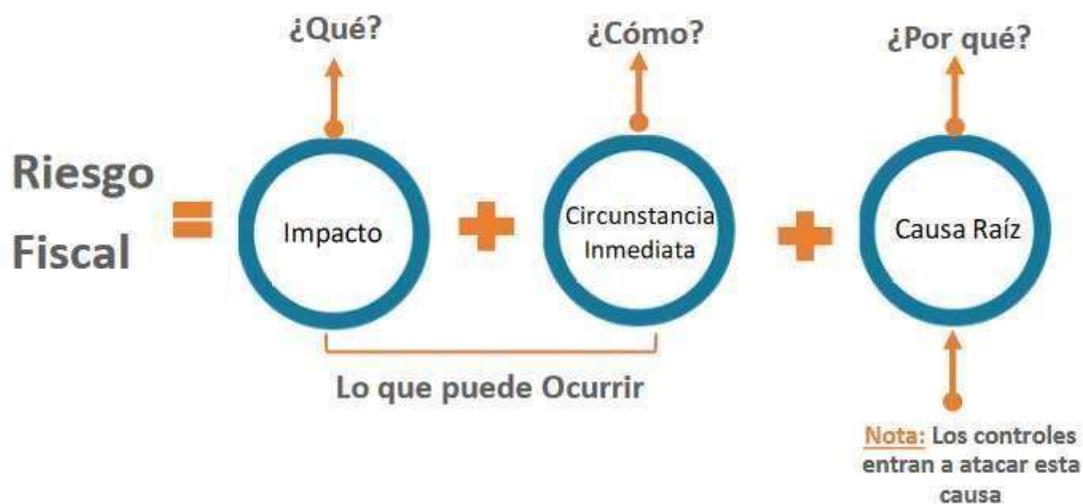
	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		POLITICA DE ADMINISTRACIÓN DEL RIESGO	
		Fecha: 03/12/2024	
		Página: 23 de 39	

Reducir el riesgo	<p>El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.</p> <p>Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.</p> <p>Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.</p>
Aceptar el riesgo	<p>No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo (Gestión y Fiscales)</p> <p>Importante: Ningún riesgo de corrupción debe ser aceptado.</p>

10.1.9. Directrices para la redacción de los Riesgos Fiscales

Para la redacción de un riesgo Fiscal es necesario tener en cuenta que se debe iniciar la oración como “Posibilidad de” debido a que es un evento potencial, posteriormente se describe el impacto que se refiere al efecto dañoso sobre los bienes y/o intereses patrimoniales de la naturaleza pública, seguido de la circunstancia inmediata que indica la situación por la que se presenta el riesgo pero no es la causa raíz y por último se describe la causa raíz que corresponde al porqué de la situación que es el evento (acción u omisión) que genera directamente el riesgo.

Ilustración 5. Redacción de un riesgo Fiscal



Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 24 de 39	

10.2. Tratamiento Riesgos de Corrupción

Teniendo en cuenta que el Gobierno Nacional viene impulsando y desarrollando diferentes políticas públicas con miras a disminuir los niveles de corrupción en todos los ámbitos, la Secretaría de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011 diseñó una metodología para que todas las entidades determinen su Plan Anticorrupción y de Atención al ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción.

Entendiendo que los riesgos de corrupción se convierten en una tipología de riesgos que debe ser controlada por la entidad, éstos deben incorporarse en primera instancia en el mapa de riesgos del proceso, sobre el cual se han identificado, de modo tal que el responsable o líder del mismo pueda realizar el seguimiento correspondiente, en conjunto con los riesgos de gestión propios del proceso, lo que promueve que el responsable tenga una mirada integral de todos los riesgos que pueden llegar a afectar el desarrollo de su proceso.

Generalidades:

Teniendo en cuenta las definiciones dadas frente a la corrupción, esta guía define:

- Los hechos de corrupción son inaceptables e indeseables.
- El riesgo de corrupción debería tratar de evitarse, estableciendo controles para el hecho de corrupción.
- **Elaboración:** el mapa de riesgos de corrupción lo elabora anualmente cada líder de proceso junto con su equipo de trabajo.
- **Consolidación:** la Dirección de Fortalecimiento Institucional como administradora del Sistema Integrado de Gestión, será la encargada de consolidar el mapa de riesgos de corrupción.
- **Publicación del mapa de riesgos de corrupción:** se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014. En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 25 de 39	

- **Socialización:** Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito los líderes de los procesos diseñarán las actividades o mecanismos necesarios de socialización el mapa actualizado para cada vigencia con el propósito de que funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción.

Así mismo, se adelantarán las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción, dejando la evidencia del proceso de socialización y publicación de sus resultados.

- **Ajustes y modificaciones:** Después de su publicación y durante el respectivo año de vigencia, los líderes de proceso podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el Mapa de Riesgos de Corrupción realizando la solicitud correspondiente ante la Dirección de Fortalecimiento Institucional. En este caso, deberán dejar por escrito los ajustes, modificaciones o inclusiones realizadas.
- **Monitoreo:** en concordancia con la cultura del autocontrol al interior de la Alcaldía Municipal de Ibagué, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de gestión y de corrupción, y enviarán el monitoreo a la Dirección de Fortalecimiento de conformidad con la periodicidad definida en la política de administración de Riesgos y/ en la circular de reportes de cada vigencia. En el tema concreto de los riesgos de soborno, el Oficial de Transparencia y el Equipo de Transparencia periódicamente harán monitoreo de los riesgos detectados y de los controles implementados
- **Seguimiento:** La Oficina de control interno realizará el seguimiento a la gestión de riesgos de corrupción. En este sentido, incluirá en sus procesos de auditoría interna, el análisis de las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 26 de 39	

10.2.1. Zona de riesgo y tratamiento

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de Corrupción	Muy baja, bajo Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Periodicidad bimestral de monitoreo para evitar a toda costa su materialización por parte de los procesos.
	Alta y Extrema	Se adoptan medidas para: REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. EVITAR Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
		TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad bimestral de monitoreo para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en el Módulo de Riesgos – SGI.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 27 de 39	

10.2.2. Directrices de redacción para riesgos de corrupción.

El riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. “Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013).

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



Fuente: Elaboración propia

- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.
- Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización como guía de la figura 13 lineamientos descripción riesgo de corrupción.

IMPORTANTE: Los riesgos de corrupción y/o soborno, siempre deben gestionarse.

Nota: Para el tratamiento de los riesgos de corrupción o soborno asociados a los tramites y servicios usar el protocolo para la identificación de riesgos.

Las fuentes ilegales de la corrupción:

- ✓ Cohecho.
- ✓ Concusión.

Otras formas de corrupción asociadas al comportamiento inmoral:

En especial para las organizaciones privadas, pueden ser tipos de corrupción asociadas a “malos” comportamientos, algunos casos, por ejemplo:

- ✓ Alteración de propuestas comerciales.
- ✓ Abstención de presentación correcta de ofertas.
- ✓ Afectación deliberada de la buena reputación.
- ✓ Afectación de licencias de funcionamiento por abstención de cumplir las obligaciones

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 28 de 39	

10.3 Tratamiento Riesgos de Seguridad y Salud en el Trabajo

Una vez se identifican los peligros y se valoran los riesgos, la entidad debe definir el tratamiento para cada uno de los riesgos identificados y evaluados de acuerdo a la **Guía para la Identificación de los Peligros y la Valoración de los Riesgos en Seguridad y Salud Ocupacional – Guía Técnica Colombiana GTC 45**, podrán ajustar estos lineamientos a sus necesidades, tomando en cuenta su naturaleza, el alcance de sus actividades y los recursos establecidos.

10.3.1 Identificación de los peligros y valoración de los Riesgos

El propósito general de la identificación de los peligros y la valoración de los riesgos en Seguridad y Salud en el trabajo (SST), es entender los peligros que se pueden generar en el desarrollo de las actividades, con el fin de que la organización pueda establecer los controles necesarios, al punto de asegurar que cualquier riesgo sea aceptable.

La valoración de los riesgos es la base para la gestión proactiva de SST, liderada por la alta dirección como parte de la gestión integral del riesgo, con la participación y compromiso de todos los niveles de la organización y otras partes interesadas. Independientemente de la complejidad de la valoración de los riesgos, ésta debería ser un proceso sistemático que garantice el cumplimiento de su propósito.

Todos los trabajadores deberían identificar y comunicar a su empleador los peligros asociados a su actividad laboral. Los empleadores tienen el deber legal de evaluar los riesgos derivados de estas actividades laborales.

El procedimiento de valoración de riesgos que se describe en esta guía está destinado a ser utilizado en:

- situaciones en que los peligros puedan afectar la seguridad o la salud y no haya certeza de que los controles existentes o planificados sean adecuados, en principio o en la práctica;
- organizaciones que buscan la mejora continua del Sistema de Gestión del S y SO y el cumplimiento de los requisitos legales, y

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 29 de 39	

- situaciones previas a la implementación de cambios en sus procesos e instalaciones.

La metodología utilizada para la valoración de los riesgos debería estructurarse y aplicarse de tal forma que ayude a la organización a:

- identificar los peligros asociados a las actividades en el lugar de trabajo y valorar los riesgos derivados de estos peligros, para poder determinar las medidas de control que se deberían tomar para establecer y mantener la seguridad y salud de sus trabajadores y otras partes interesadas;
- tomar decisiones en cuanto a la selección de maquinaria, materiales, herramientas, métodos, procedimientos, equipo y organización del trabajo con base en la información recolectada en la valoración de los riesgos;
- comprobar si las medidas de control existentes en el lugar de trabajo son efectivas para reducir los riesgos;
- priorizar la ejecución de acciones de mejora resultantes del proceso de valoración de los riesgos, y
- demostrar a las partes interesadas que se han identificado todos los peligros asociados al trabajo y que se han dado los criterios para la implementación de las medidas de control necesarias para proteger la seguridad y la salud de los trabajadores.

10.3.2 Aspectos para tener en cuenta al desarrollar la identificación de los peligros y la valoración de los Riesgos

Para que la identificación de los peligros y la valoración de los riesgos sean útiles en la práctica, las organizaciones deberían:

- a) designar un miembro de la organización y proveer los recursos necesarios para promover y gestionar la actividad;
- b) tener en cuenta la legislación vigente y otros requisitos;
- c) consultar con las partes interesadas pertinentes, comunicarles lo que se ha

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 30 de 39	

planificado hacer y obtener sus comentarios y compromisos;

- d) determinar las necesidades de entrenamiento del personal o grupos de trabajo para la identificación de los peligros y la valoración de los riesgos e implementar un programa adecuado para satisfacerlas;
- e) documentar los resultados de la valoración;
- f) realizar evaluaciones higiénicas y/o monitoreos biológicos, si se requiere;
- g) tener en cuenta los cambios en los procesos administrativos y productivos, procedimientos, personal, instalaciones, requisitos legales y otros;
- h) tener en cuenta las estadísticas de incidentes ocurridos y consultar información de gremios u organismos de referencia en el tema;

10.3.3 Actividades para identificar los Peligros y Valorar los Riesgos

Las siguientes actividades son necesarias para que las organizaciones realicen la identificación de los peligros y la valoración de los riesgos (véase la Figura 1):

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Versión: 11	
		Fecha: 03/12/2024	
		Página: 31 de 39	

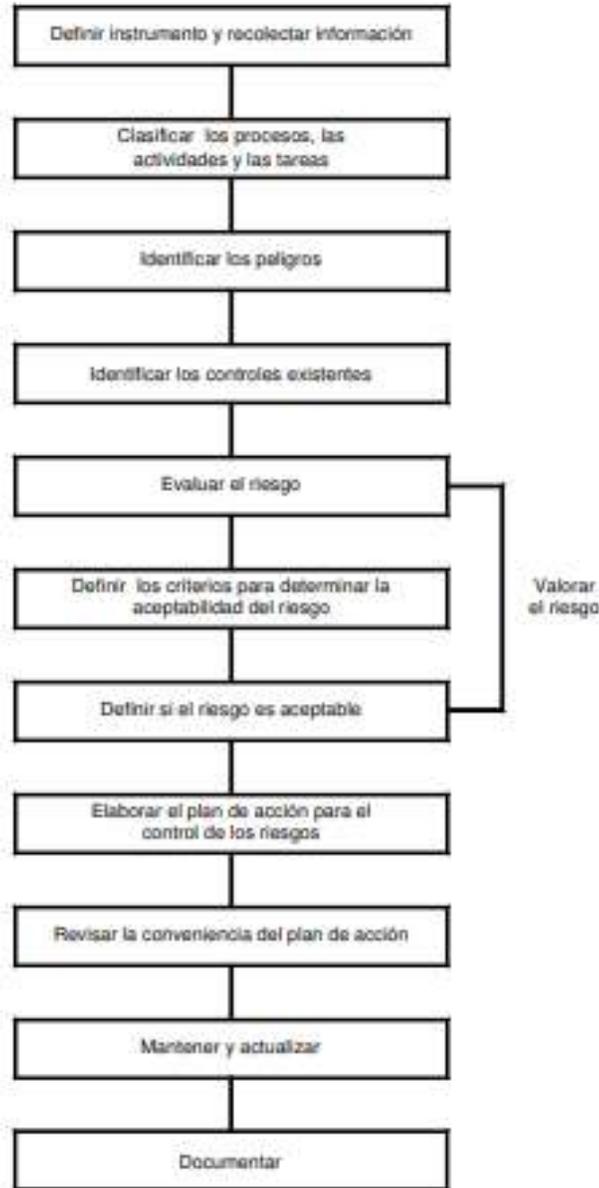


Figura 1. Actividades para identificar los peligros y valorar los riesgos

- a) Definir el instrumento para recolectar la información: una herramienta donde se registre la información para la identificación de los peligros y valoración de los riesgos. Un ejemplo de una herramienta de este tipo se presenta en el Anexo B.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		POLITICA DE ADMINISTRACIÓN DEL RIESGO	
		Fecha: 03/12/2024	
		Página: 32 de 39	

ANEXO B
(Informativo)

MATRIZ DE RIESGOS

A continuación se presentan dos ejemplos de los elementos que podría contener una matriz de riesgo.

Proceso Zona / Lugar	Actividades	Tareas Rutinario (S o No)	Peligro		Efectos posibles	Controles existentes			Evaluación del riesgo						Valores del riesgo	Criterios para establecer controles		Medidas Intervención					
			Descripción	Clasificación		Fuente	Medio	Individuos	Nivel de Detención a	Nivel de Exposición	Nivel de Probabilidad (Riesgo)	Interpretación del nivel de probabilidad	Nivel de Consecuencia	Nivel de Impacto (M) e intención		Interpretación del IR	Aceptabilidad del riesgo	No Efectivos	Prior Competencia	El agente Requiere Protección Asociada (S o No)	Eliminación	Substitución	Controles de Ingeniería
Ejemplo 1																							
Mantenimiento Obras de Conectividad y Conexión Mantenimiento Técnico de OBRAS de ALTA TENSION	Pintar Paredes	Si	Manejo Inadecuado de herramientas manuales	Mecánico	Heridas, golpes	Ninguno	Inspecciones de herramientas	Ninguno	3	4	8	MEDIO	25	2000	8	No	6	Contacas, Contusiones	Si			Generar y aplicar de un análisis de trabajo seguro (ATS) previo a la ejecución de una tarea.	Dotar a los trabajadores de guantes para protección de acuerdo al estándar de protección establecido por la organización.
			Exposición a gases y vapores	Químico	Iritación de la vía respiratoria y mucosas	Ninguno	Ninguno	Uso de tapabocas	5	4	24	MUY ALTO	25	6000	8	No	6	Afecciones Respiratorias	Si	Uso de pinturas a base de agua donde sea aplicable.	Uso de ventiladores portátiles.		Dotar a los trabajadores con respiradores con filtro de gases de acuerdo al agente al cual está expuesto.

EJEMPLO 1 Valoración de riesgos asociados a una organización que se dedica a la pintura de instalaciones locativas.

- b) Clasificar los procesos, las actividades y las tareas: preparar una lista de los procesos de trabajo y de cada una de las actividades que lo componen y clasificarlas; esta lista debería incluir instalaciones, planta, personas y procedimientos.
- c) Identificar los peligros: incluir todos aquellos relacionados con cada actividad laboral. Considerar quién, cuándo y cómo puede resultar afectado.
- d) Identificar los controles existentes: relacionar todos los controles que la organización ha implementado para reducir el riesgo asociado a cada peligro.
- e) Valorar riesgo

Evaluar el riesgo: calificar el riesgo asociado a cada peligro, incluyendo los controles existentes que están implementados. Se debería considerar la eficacia de dichos controles, así como la probabilidad y las consecuencias si éstos fallan.

- Definir los criterios para determinar la aceptabilidad del riesgo.
- Definir si el riesgo es aceptable: determinar la aceptabilidad de los riesgos y decidir si los controles de S y SO existentes o planificados son suficientes para mantener los riesgos bajo control y cumplir los requisitos legales.
- f) Elaborar el plan de acción para el control de los riesgos, con el fin de mejorar los controles existentes si es necesario, o atender cualquier otro asunto que lo requiera.
- g) Revisar la conveniencia del plan de acción: re-valorar los riesgos con base en los controles propuestos y verificar que los riesgos serán aceptables.
- h) Mantener y actualizar:
 - realizar seguimiento a los controles nuevos y existentes y asegurar que sean efectivos;
 - asegurar que los controles implementados son efectivos y que la valoración de los

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 33 de 39	

riesgos está actualizada.

- i) Documentar el seguimiento a la implementación de los controles establecidos en el plan de acción que incluya responsables, fechas de programación, ejecución y estado actual, como parte de la trazabilidad de la gestión en S y SO.

10.3.4 Descripción y clasificación de los Peligros

Para identificar los peligros, se recomienda plantear una serie de preguntas como las siguientes:

- ¿existe una situación que pueda generar daño?
- ¿quién (o qué) puede sufrir daño?
- ¿cómo puede ocurrir el daño?
- ¿cuándo puede ocurrir el daño?

Para la descripción y clasificación de los peligros se podrá tener en cuenta la tabla del Anexo A. Este cuadro no es un listado exhaustivo. Las organizaciones deberían desarrollar su propia lista de peligros tomando en cuenta el carácter de sus actividades laborales y los sitios en que se realiza el trabajo.

ANEXO A Informativo)

Tabla de peligros

Descripción	Clasificación						
	Biológico	Físico	Químico	Psicosocial	Biomecánicos	Condiciones de seguridad	Fenómenos naturales*
Virus	Ruido (de impacto, intermitente, continuo)	Polvos orgánicos e inorgánicos	Gestión organizacional (estilo de mando, pago, contratación, participación, inducción y capacitación, bienestar social, evaluación del desempeño, manejo de cambios).	Postura (prolongada mantenida, forzada, antigraavitacional)	Mecánico (elementos o partes de máquinas, herramientas, equipos, piezas a trabajar, materiales proyectados sólidos o fluidos)	Sismo	
Bacterias	Iluminación (luz visible por exceso o deficiencia)	Fibras	Características de la organización del trabajo (comunicación, tecnología, organización del trabajo, demandas cualitativas y cuantitativas de la labor).	Esfuerzo	Eléctrico (alta y baja tensión, estática)	Terremoto	
Hongos	Vibración (cuerpo entero, segmentaria)	Líquidos (nieblas y rocíos)	Características del grupo social de trabajo (relaciones, cohesión, calidad de interacciones, trabajo en equipo).	Movimiento repetitivo	Locativo (sistemas y medios de almacenamiento), superficies de trabajo (irregulares, deslizantes, con diferencia del nivel), condiciones de orden y aseo, (caídas de objeto)	Vendaval	
Rickettsias	Temperaturas extremas (calor y frío)	Gases y vapores	Condiciones de la tarea (carga mental, contenido de la tarea, demandas emocionales, sistemas de control, definición de roles, monotonía, etc).	Manipulación manual de cargas	Tecnológico (explosión, fuga, derrame, incendio)	Inundación	
Parásitos	Presión atmosférica (normal ajustada) y	Humos metálicos, no metálicos	Interfase persona - tarea (conocimientos, habilidades en relación con la demanda de la tarea, iniciativa, autonomía y reconocimiento, identificación de la persona con la tarea y la organización).		Accidentes de tránsito	Derrumbe	
Picaduras	Radiaciones ionizantes (rayos x, gama, beta y alfa)	Material particulado	Jornada de trabajo (pausas, trabajo nocturno, rotación, horas extras, descansos)		Públicos (robos, atracos, asaltos, atentados, de orden público, etc.)	Precipitaciones, (lluvias, granizadas, heladas)	
Mordeduras	Radiaciones no ionizantes (láser, ultravioleta, infrarroja, radiofrecuencia, microondas)				Trabajo en alturas		
Fluidos o excrementos					Espacios confinados		

* Tener en cuenta únicamente los peligros de fenómenos naturales que afectan la seguridad y bienestar de las personas en el desarrollo de una actividad. En el plan de emergencia de cada empresa, se considerarán todos los fenómenos naturales que pudieran afectarla.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 34 de 39	

10.4 Tratamiento Riesgos de Seguridad Digital

Una vez se han identificado los riesgos, la entidad pública debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional.

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener en cuenta las opciones planteadas en la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” del DAFP: **Evitar, aceptar, compartir o mitigar el riesgo.**

10.4.1 Planes de Tratamiento de Riesgos de Seguridad Digital e Indicadores para la gestión del Riesgo

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el **Esquema 9. Consolidación de los Planes de Tratamiento de Riesgos**, de la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” emitida por el DAFP

Importante:

Si la entidad pública decide **mitigar o tratar el riesgo** mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la **Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA**, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad digital, sin embargo, la entidad pública puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

10.4.2 Fase 2. Ejecución

Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la **Fase 1**.

Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (**Primer Línea de Defensa** y la **Oficina de Tecnologías de la Información -TI**

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 35 de 39	

generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

10.4.3 Fase 3. Monitoreo y Revisión

El monitoreo y revisión se realiza cumpliendo los lineamientos establecidos en el numeral 9 Roles y Responsabilidades de las **Líneas de defensa** y que a su vez se encuentran definidas en el Manual de MIPG.

10.4.4 Reporte de la gestión del riesgo de seguridad digital al interior de la entidad pública

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:



Imagen 3. Reportes de información por parte de la entidad.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 36 de 39	

10.4.5 Auditorías internas y externas

Le corresponde a las **Unidades de Control Interno (tercera línea de defensa)**, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad digital en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

10.4.6 Medición del Desempeño

La entidad pública debe utilizar medidas de desempeño (indicadores) para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica

10.4.7 Fase 4. Mejoramiento continuo de la gestión del riesgo de Seguridad Digital

La entidad pública debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad digital de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Empezar acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 37 de 39	

11. Riesgos de Seguridad y Salud en el trabajo.

La identificación y tratamiento de riesgos de seguridad y salud en el trabajo en la Alcaldía Municipal de Ibagué se realiza bajo adopción e implementación de la Guía Técnica Colombiana para identificación de los peligros y valoración de los riesgos de seguridad y salud ocupacional GTC 45.

La metodología se encuentra descrita en el Procedimiento identificación de peligros evaluación y valoración del riesgo IPEVR, publicado en la página web de la entidad.

12. Riesgos Ambientales.

La identificación y tratamiento de riesgos ambientales en la Alcaldía Municipal de Ibagué se realiza bajo la adopción e implementación de la Guía Técnica Colombiana Gestión del Riesgo Ambiental GTC 104.

La metodología se encuentra descrita en el Procedimiento identificación de aspectos y valoración de impactos ambientales, publicado en la página web de la entidad.

13. Comunicación y consulta

La comunicación y consulta con las partes involucradas tanto internas como externas debe desarrollarse durante todas las etapas del proceso para la gestión del riesgo.

Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios.

Así mismo es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 38 de 39	

14. Control de cambio

Versión	Vigente desde	Descripción del Cambio
01	11/12/2015	Primera Versión SIGAMI.
02	22/08/2017	Modificación por cambio en la metodología DAFP.
03	4/10/2018	Modificación por cambio en la metodología del DAFP
04	26/11/2018	Inclusión de los criterios para calificar impactos por riesgos de corrupción.
05	15/05/2019	Se actualizo nombre del Proceso de acuerdo a los nuevos sistemas que conforman el Sistema de Gestión de la Alcaldía Municipal.
06	30/10/2019	Se adopta dentro de la metodología de la política de administración del Riesgo el manual emitido por Colombia Compra Eficiente "Manual para la identificación y cobertura del riesgo en los procesos de contratación".
07	5/12/2020	Se incluye actualización de los roles de las líneas de defensa.
08	25/02/2022	<ul style="list-style-type: none"> - Se adopta la nueva guía del Departamento Administrativo de la Función Pública " Guía para la administración de riesgos y el diseño de controles en entidades públicas. - Se incluyen los riesgos de soborno. - Se actualizan las responsabilidades de la segunda línea de defensa teniendo en cuenta el mapa de aseguramiento institucional.
09	28-10-2022	<ul style="list-style-type: none"> - Ajuste al numeral 8.1 lineamientos operativos. - Ajuste al numeral 9, responsables de las líneas de defensa. - Ajuste a la valoración del impacto numeral 10.1.3. - Incluye numeral nuevo 8.4 seguimiento.
10	22/12/2023	<ul style="list-style-type: none"> - Cambio de versión de la guía de administración del riesgo y diseño de controles en entidades públicas, se incluye lineamientos para el análisis del riesgo fiscal. - Se incluye numeral 10.1.9. Directrices para redacción de riesgo fiscal.

	SISTEMA INTEGRADO DE GESTIÓN Y MIPG	Código: POL-SIG-01	
		Versión: 11	
	POLITICA DE ADMINISTRACIÓN DEL RIESGO	Fecha: 03/12/2024	
		Página: 39 de 39	

11	16/12/2024	<ul style="list-style-type: none"> - Se actualizó numeral 7.1 Metodología a utilizar, incluyendo Seguridad de la Información - Ajuste numeral 9. Roles y Responsabilidades, para la Administración del Riesgo por Procesos, definidos en la Entidad, líneas de defensa 1,2,3 responsable, Responsabilidad frente al cargo, de acuerdo con el Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5. - Incluye numeral nuevo 10.3 Tratamiento de Riesgos de Seguridad y Salud en el Trabajo. - Incluye numeral nuevo 10.4 Tratamiento de Riesgos de Seguridad Digital.
----	------------	---

15. Ruta de Aprobación

Elaboró	Revisó	Aprobó
Director(a) de Fortalecimiento Institucional	Secretario(a) de Planeación	Comité de Coordinación de Control Interno