



Política para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital

Versión 4 – Ciudad de Itagüí



Alcaldía
de Itagüí



POLÍTICA PARA LA GESTIÓN DE LOS RIESGOS

POLÍTICA PARA LA GESTIÓN DE LOS RIESGOS

Política para la Gestión de los Riesgos y el Diseño de Controles – Versión 4
Aprobada por: Comité Coordinador de Control Interno
Acta N° 01 de 2024
Decreto N.º 509 del 17 de abril de 2020

CONTENIDO

INTRODUCCIÓN	4
TERMINOS Y DEFINICIONES.....	5
1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.	8
1.1 Objetivo general	8
1.2 Alcance	8
1.3 Estructura para la Gestión del Riesgo.....	8
1.4 Metodología para la Administración del Riesgo	9
2. IDENTIFICACIÓN DEL RIESGO	9
2.1 Análisis de Objetivos Estratégicos y de los Procesos:	9
2.2 Identificación de los puntos de riesgo:	9
2.3 Identificación de áreas de impacto:.....	10
2.4 Identificación de Áreas de Factores de Riesgo:	10
2.5 Descripción del riesgo:.....	10
2.6 Clasificación del Riesgo:	11
3. VALORACIÓN DEL RIESGO.....	11
3.1 Análisis Del Riesgo	11
3.2 Evaluación del Riesgos:.....	12
3.3 Estrategias para tratar el Riesgo:.....	15
3.4 Herramientas para la Gestión del Riesgo:.....	16
3.5 Monitoreo y Revisión:.....	16
4. LINEAMIENTOS PARA EL ANALISIS DE RIESGO FISCAL.....	18
5. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN	19
6. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	23
6.1 Identificación de los activos de seguridad de la información.....	23
6.2 Identificación del riesgo.....	24
7. CONTROL DE CAMBIOS:.....	25

INTRODUCCIÓN

El municipio de Itagüí define su política de riesgos tomando como referencia el Modelo Integrado de Planeación y Gestión (MIPG), las directrices de las políticas de gestión y desempeño y el esquema de líneas de defensa como elemento del Modelo Estándar de Control Interno (MECI) y los lineamientos de la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública, vigente, en consonancia con la normatividad aplicable a la entidad y al Sistema Integrado de Gestión.

Siendo esta una declaración de la alta dirección, la política de administración de riesgos plasma el compromiso y las intenciones generales de la administración municipal definidas en su marco estratégico y en la planeación institucional, considerando el enfoque de procesos y la planeación de los mismos (planes, programas o proyectos asociados), estableciendo lineamientos precisos acerca del tratamiento, manejo y seguimiento a los eventos potenciales que pueden generar efecto sobre los objetivos Institucionales, mediante un ámbito estratégico y tres líneas de defensa, soportándose en los mecanismos de comunicación disponibles y cubriendo las responsabilidades de la Entidad y las de cada proceso.

Establece además una estructura para la formulación y el análisis de los controles, definiendo atributos en relación con su diseño y ejecución, procurando la eficacia de los mismos y facilitando su implementación por parte de los responsables; definiendo criterios respecto al tratamiento de los riesgos identificados a fin de mitigar los efectos negativos en las metas institucionales; direccionando la forma de gestionar los riesgos institucionales, unificando un lenguaje común sobre el tema, así como el establecimiento de criterios que permitan la sostenibilidad de la administración del riesgo.

De acuerdo con lo anterior, a través del presente documento se presenta la declaración con respecto a la gestión de los riesgos, definiendo los lineamientos acerca del tratamiento, manejo y seguimiento.

TERMINOS Y DEFINICIONES

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.

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

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.

Ejemplos: Las calles, plazas, puentes, vías, parques etc.

b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.

Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. **Nota:** Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata).

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

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

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: medida que permite reducir o mitigar un riesgo.

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar,

prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

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

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

Factores de Riesgo: Son las fuentes generadoras de riesgos.

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.

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.

Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares

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 fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

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

Tratamiento del riesgo: consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

Valoración del riesgo: busca identificar y analizar los riesgos que enfrenta la entidad, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos.

1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.

“La Administración Municipal de Itagüí, se compromete a diseñar y aplicar herramientas que permitan fortalecer la identificación, gestión y evaluación de los riesgos aplicando estrategias de prevención y control para el tratamiento de los riesgos que puedan afectar los objetivos institucionales, proporcionando a la entidad un aseguramiento razonable con respecto al logro de los mismos, aumentando la capacidad para lograr los resultados, previniendo, reduciendo o eliminando los efectos indeseados”.

1.1 Objetivo general

Definir la metodología para la Gestión de los riesgos en la Administración Municipal de Itagüí, con un enfoque preventivo que permita a la entidad la identificación de los riesgos y la definición de acciones y estrategias institucionales a desarrollar frente a los eventos o situaciones susceptibles de impactar de manera negativa en el cumplimiento de la misionalidad y el logro de los objetivos institucionales disminuyendo de esta manera las vulnerabilidades y sus consecuencias ante amenazas internas y externas, mejorando la capacidad institucional de respuesta a eventos identificados o inesperados que afecten el talento humano, la infraestructura, los bienes o los servicios esenciales para la Entidad.

1.2 Alcance

La Política de Administración de Riesgos de la Administración Municipal de Itagüí, es aplicable al direccionamiento estratégico de la entidad, a los procesos, a los planes institucionales, a los proyectos y a las acciones ejecutadas por los servidores públicos durante el ejercicio de sus funciones y particulares que ejerzan funciones públicas en la entidad; dándoles el tratamiento necesario, con base en la metodología definida, para cada tipología de riesgos.

1.3 Estructura para la Gestión del Riesgo

Secretaría de Evaluación y Control (3era Línea de Defensa): Define la Política para la Gestión de los riesgos institucionales, realiza el seguimiento, evaluación y los reportes a los usuarios y partes interesadas.

Comité Institucional de Gestión y Desempeño: Analiza la Gestión de los Riesgos y las mejoras para su gestión

Comité Coordinador de Control Interno: Analiza los eventos y riesgos críticos (Mapa de Riesgos Institucional).

Departamento Administrativo de Planeación (2da Línea de Defensa): Define la metodología para la gestión de los Riesgos, acompaña la gestión y el seguimiento a los mismos, identificando oportunidades de mejoramiento.

Líderes de Procesos (1era línea de defensa): Gestionan los riesgos, realizan seguimiento y control a los mismos.

Enlaces MIPG: Personas claves en las Unidades Administrativas que ayudan a los líderes de los procesos y se articulan con la 2da línea de defensa para la gestión de los riesgos.

Servidores Públicos: Ejecutan los controles y acciones para la gestión de los riesgos de manera permanente.

1.4 Metodología para la Administración del Riesgo

Para gestionar el riesgo, es importante considerar lo establecido en el modelo integrado de planeación y gestión (MIPG), el cual tiene como fin generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio y muy especialmente la “política de planeación institucional” de la dimensión “Direccionamiento estratégico y planeación” del MIPG, además del conocimiento la plataforma estratégica de la entidad, la cual tiene como componentes la misión, la visión, los objetivos estratégicos y la planeación institucional; también se debe conocer el modelo de operación por procesos incluyendo su cadena de valor (Caracterizaciones), al igual que el objetivo de cada uno de los procesos, los planes, programas y proyectos asociados a cada uno de estos, identificando las metas a largo mediano y corto plazo.

2. IDENTIFICACIÓN DEL RIESGO

Para identificar los riesgos se debe tener en cuenta: El análisis contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

2.1 Análisis de Objetivos Estratégicos y de los Procesos

Analizar los objetivos estratégicos identificando los posibles eventos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso; verificando además su alineación con la Misión y la Visión institucional, así como su adecuada formulación, es decir, que contengan las Sigüientes características mínimas: específicos, medibles, alcanzables, relevantes y proyectados en el tiempo.

2.2 Identificación de los puntos de riesgo

Analizar el contenido del proceso, identificando donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo que deban mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

2.3 Identificación de áreas de impacto

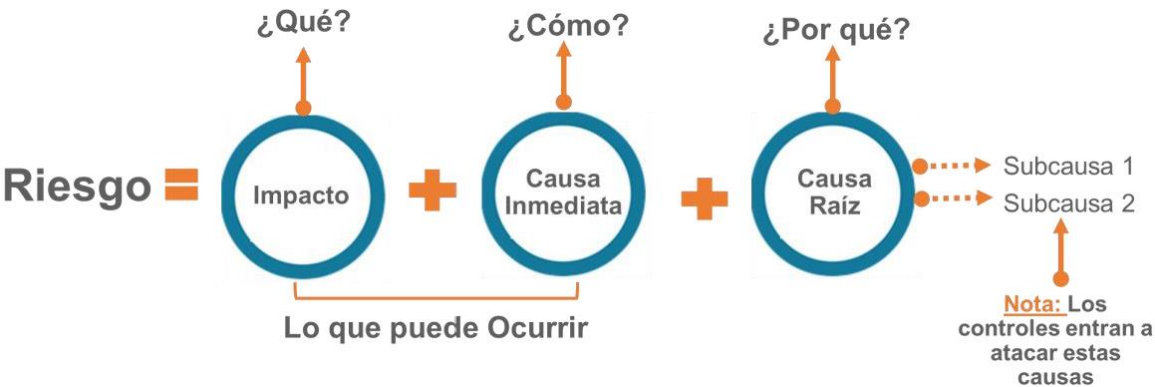
El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo.

2.4 Identificación de Áreas de Factores de Riesgo

Son las fuentes generadoras de riesgos, se identifican usando el formato FO-DE-09 Análisis del contexto estratégico de la entidad, teniendo en cuenta las cuestiones Externas, Internas y de los procesos, que se ejecutan en cada unidad administrativa, de acuerdo con la complejidad propia, el entorno en el que se desenvuelve u otros aspectos que puedan llegar a ser pertinentes.

2.5 Descripción del riesgo

La descripción del riesgo debe contener la Siguiete estructura, la cual facilita la redacción del riesgo y la claridad del mismo, inicia con la frase POSIBILIDAD DE y se analizan los Siguietes aspectos:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

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

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

2.6 Clasificación del Riesgo

Una vez identificados los riesgos se clasifican cada uno dentro de las Sigüientes 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. Eventos externos como atentados, vandalismo, orden público.
Tecnológicos	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Talento Humano	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.
De servicios	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Activos fijos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros.
Corrupción o 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 están involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

3. VALORACIÓN DEL RIESGO

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

3.1 Análisis del Riesgo

Este análisis tiene como objetivo establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo.

Para efectos de este análisis, 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**.

Bajo este esquema, se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad.

La **exposición al riesgo** estará asociada al proceso o actividad que se esté analizando, es decir, al **número de veces que se pasa por el punto de riesgo en el periodo de 1 año**, en la Siguiete tabla se establecen los criterios para definir el nivel de probabilidad.

Criterios para definir el nivel de probabilidad

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Determinar el impacto

Se definen los factores económicos y reputacionales como las variables que determinan el impacto, cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

En la Siguiete tabla se establecen los criterios para definir el nivel de impacto.

Criterios para definir el nivel de impacto

	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de alta dirección 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 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

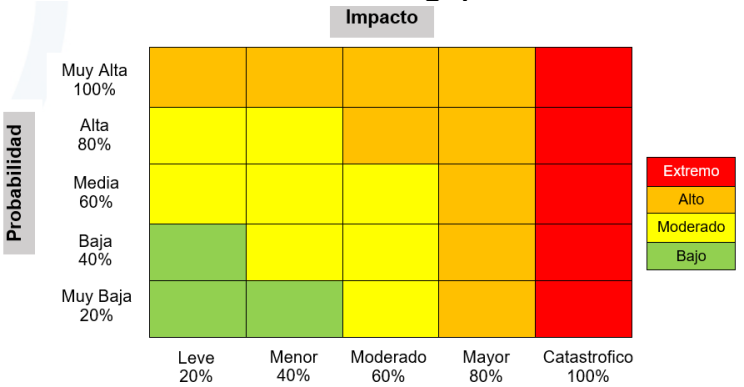
3.2 Evaluación del Riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se 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.

Matriz de calor (niveles de severidad del riesgo)



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Valoración de controles: Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo.
- La implementación y monitoreo los controles corresponde a los líderes de proceso y equipos de trabajo.

Estructura para la descripción del control:



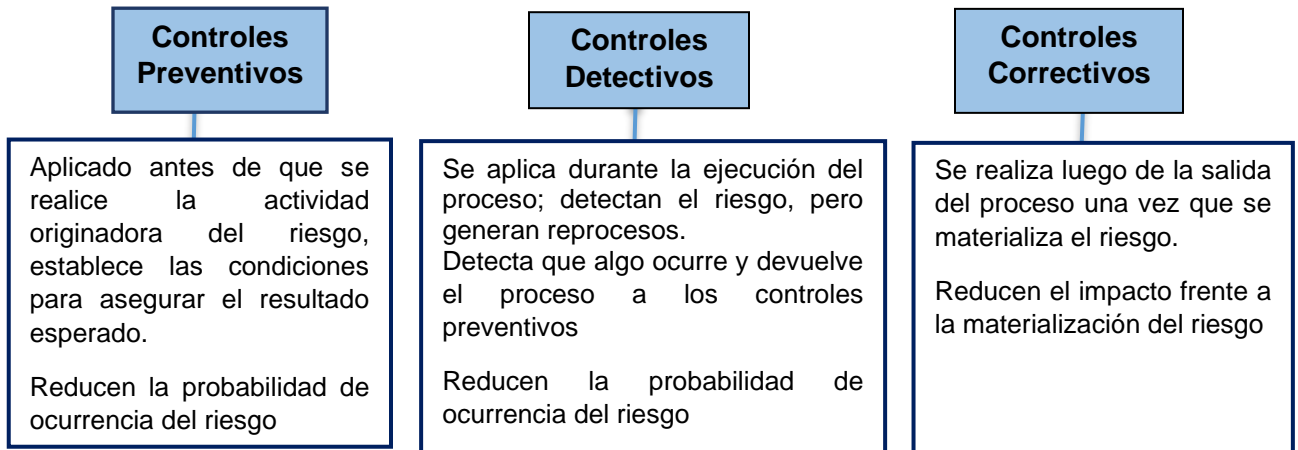
Responsable: debe tener definido el responsable de realizar la actividad de control.

Acción: Indica la actividad de control que se realiza.

Complemento: corresponde a los detalles para la efectividad del control como:

- **Periodicidad:** debe tener una periodicidad definida para su ejecución.
- **Propósito:** debe indicar cuál es el propósito del control.
- **Desviaciones:** debe indicar que pasa con las observaciones o desviaciones resultantes de la ejecución el control.
- **Evidencia:** **Debe referenciar la evidencia o registro de la ejecución del control:** Los controles deben estar previamente establecidos y referenciados en la información documentada de los procesos.

Tipos de controles:



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

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.

Análisis y evaluación de los controles: en la siguiente tabla se determinan los atributos y pesos asociados para el análisis del control:

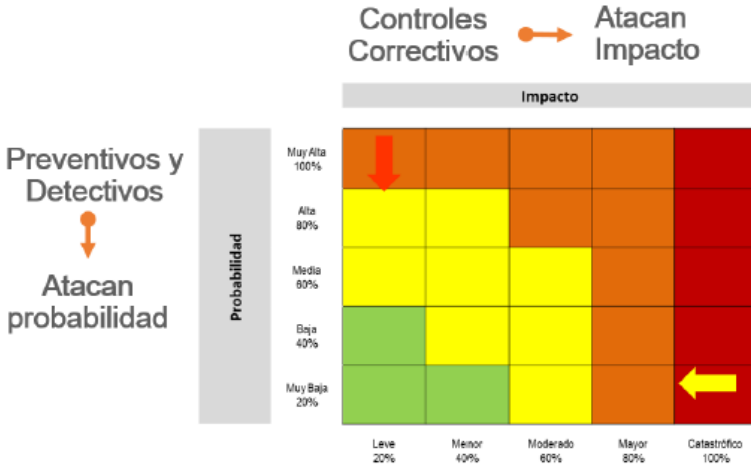
Atributos de para el diseño del control

Características		Descripción		Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Los controles deben estar documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-

Características		Descripción	Peso	
		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.	-

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

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



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente.

3.3 Estrategias para tratar el Riesgo

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser reducir, mitigar, transferir, evitar o aceptar. 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: Después de realizar un análisis y considerar los niveles de riesgo, se implementan acciones que reduzcan la probabilidad de riesgo.

Transferir: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad Reputacional.

Evitar: Después de realizar análisis y considerar que el nivel de riesgo es demasiado alto, se determina no asumir la actividad que genera este riesgo, o asumirla en condiciones controladas.

Para el tratamiento del riesgo, se requiere la definición de un plan de acción que especifique: las acciones a implementar, el responsable, fecha de implementación, y fecha de seguimiento.

Nota: El plan de acción acá referido es diferente al “plan de contingencia” y se considera un control correctivo enfocado a la Mitigación de los efectos como consecuencia de la materialización del riesgo.

3.4 Herramientas para la Gestión del Riesgo

El municipio de Itagüí determina y dispone mediante el proceso de Direccionamiento Estratégico del SGI, los Instrumentos necesarios para identificar, medir, valorar, monitorear, evaluar y administrar los riesgos, identificando los requerimientos funcionales; revisa periódicamente su adecuado funcionamiento y requerimientos de información y dispone una matriz de Riesgos para el uso en todas las Unidades Administrativas y los procesos.

[\\10.1.10.2\SGI\1. DIRECCIONAMIENTO ESTRATÉGICO\Formatos SGI – Intranet Alcaldía de Itagüí \(itagui.gov.co\)](#)

Para una mayor comprensión de la política de operación para la administración del riesgo, se define que los anexos son parte fundamental de este documento técnico, por tanto, se recomienda su consulta y conocimiento por parte de todos los servidores públicos de la Entidad.

- Manual operativo MIPG
- Guía para la Administración del riesgo del DAFP versión vigente
- PR-DE-05 Procedimiento para la Gestión de los riesgos, oportunidades y Ac preventivas
- FO-DE-09 Análisis del Contexto Estratégico
- FO-DE-11 Matriz de Riesgos
- FO-DE-12 Matriz de Identificación de Peligros y Valoración de Riesgos en SST
- FO-DE-17 Análisis y Evaluación de los Controles

3.5 Monitoreo y Revisión

El Modelo Integrado de Planeación y Gestión (MIPG) desarrolla en la dimensión 7 “*control interno*”, las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad, (Ver Anexo 1):

Los riesgos deben ser incluidos en la Matriz de Riesgos por Unidad administrativa y por proceso, independiente del nivel de valoración, Adicionalmente, para los niveles moderado, alto o extremo se deberán documentar al interior de los procesos acciones de contención (antes de que ocurra el evento) y de contingencia siempre que ocurra el evento para tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación de los servicios; estos planes estarán documentados en la matriz de riesgos para cada proceso y en los planes de mejoramiento y podrán ser consultados en el mapa de riesgos de la entidad.

Anualmente se revisa el mapa de riesgos completo de la Entidad, para lo cual se toma como insumo, las auditorías Internas realizadas por la Secretaría de Evaluación y Control, las auditorías de Calidad y las auditorías realizadas por Órganos de Control, así como la información reportada en los seguimientos de la matriz de riesgos e informes de desempeño presentados por los líderes de procesos, en los plazos establecidos y el Mapa de Riesgos de Corrupción de acuerdo a lo establecido dentro del Plan Anticorrupción y de Atención al ciudadano de cada vigencia.

NIVEL	REGISTRO	SEGUIMIENTO
EXTREMO	Matriz de Riesgos Planes de mejoramiento y/o Desempeño de los procesos Informes presentados a la Dirección	Trimestral con Reporte inmediato en caso de presentarse
ALTO	Matriz de Riesgos Planes de mejoramiento y/o Desempeño de los procesos	Trimestral
MODERADO	Matriz de Riesgos Planes de mejoramiento y/o Desempeño de los procesos	Trimestral
BAJO	Informes de Desempeño del proceso	Semestral

La información resultante de la gestión, monitoreo y evaluación, debe ser publicada en la página Web, según los compromisos vigentes, Así:

- 31 de enero de cada año, se publica el mapa de riesgos institucional incluyendo los riesgos de seguridad de la información y el mapa de riesgos de corrupción (Departamento Administrativo de Planeación)
- 30 de abril de cada año, posterior al primer ciclo de monitoreo y evaluación al mapa de riesgos de corrupción, publicar dentro de los 20 primeros días calendario de mayo del mismo año. (Departamento Administrativo de Planeación (10 días) – Secretaría de Evaluación y Control (10 días)).
- 30 de junio de cada año, posterior al segundo ciclo de monitoreo y evaluación al mapa de riesgos institucional, publicar dentro de los 20 primeros días de Julio del mismo año. (Departamento Administrativo de Planeación (10 días) – Secretaría de Evaluación y Control (10 días)).
- 31 de agosto de cada año, posterior al segundo ciclo de monitoreo y evaluación al mapa de riesgos de corrupción, publicar dentro de los 20 primeros días de septiembre del mismo año. (Departamento Administrativo de Planeación (10 días) – Secretaría de Evaluación y Control (10 días)).

- 31 de diciembre de cada año, posterior al tercer ciclo de monitoreo y evaluación: al mapa de riesgos de corrupción y al segundo ciclo de Seguimiento del Mapa de Riesgos Institucional, publicar dentro de los 20 primeros días de enero del Siguiete año. (Departamento Administrativo de Planeación (10 días) – Secretaría de Evaluación y Control (10 días)).

4. LINEAMIENTOS PARA EL ANALISIS DE RIESGO FISCAL

La finalidad de este acápite es prevenir la constitución de eventos generadores de responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado.

Paso a paso para la definición del mapa de riesgos fiscales:

- **Identificación de riesgos fiscales:**
Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.
- **Identificación de áreas de impacto:**
Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

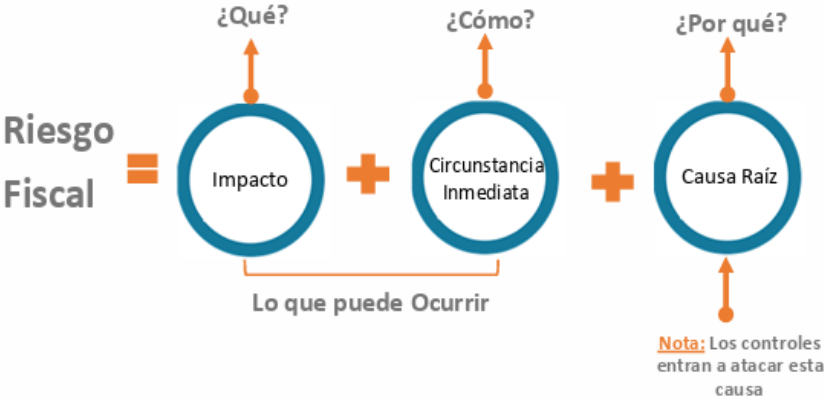
Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.
- **Identificación de la causa raíz o potencial hecho generador:**
La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

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

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

- Descripción del Riesgo Fiscal**

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos:



Ejemplo:

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos , por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos , por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública , por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Una vez identificados los “Riesgos Fiscales”, se gestionan conforme a los lineamientos dados en este documento, para los riesgos de Gestión.

5. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Definición del Riesgo de Corrupción

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, por lo cual es necesario que en la descripción del mismo concurren los siguientes componentes:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Con el fin de evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción antes de definirlo se debe hacer el análisis, acorde al ejemplo de la Siguiente tabla:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

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

Teniendo en cuenta que los riesgos de corrupción se establecen sobre los **procesos**.

Análisis de Probabilidad:

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	El evento puede ocurrir solo en circunstancias Excepcionales (No se ha presentado en los 5 últimos años)	1=20%
Baja	El evento puede ocurrir en algún momento (Al menos una vez en los 5 últimos años)	2=40%
Media	El evento podrá ocurrir en algún momento (al menos una vez en los 2 últimos años)	3=60%
Alta	Es viable que evento ocurra en la mayoría de las circunstancias (al menos 1 vez en el último año)	4=80%
Muy Alta	Se espera que el evento ocurra en la mayoría de las circunstancias (más de una vez al año)	5=100%

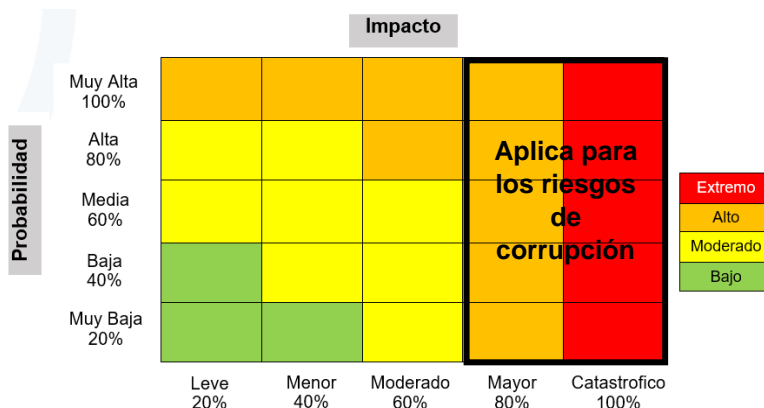
Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo y de acuerdo a la aplicación del FO-DE-11 Criterios para Calificar el Impacto de los riesgos de Corrupción, y la calificación del análisis se aplica en la matriz General.

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

Nivel de impacto MAYOR



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles, “mayor” y “catastrófico”, no aplican los niveles de impacto insignificante y menor, que sí aplican para los riesgos de Gestión dadas las consecuencias que se derivan de el para la entidad.

Tratamiento del riesgo de corrupción:

Reducir: Después de realizar un análisis y considerar los niveles de riesgo, se implementan acciones que reduzcan probabilidad y/o el impacto del riesgo de riesgo.

Evitar: Después de realizar análisis y considerar que el nivel de riesgo es demasiado alto, se determina no asumir la actividad que genera este riesgo, o asumirla en condiciones controladas.

Los Controles para el riesgo de corrupción se aplican igual que para los riesgos de gestión Para el tratamiento del riesgo, se requiere la definición de un plan de acción que especifique: las acciones a implementar, el responsable, fecha de implementación, y fecha de seguimiento.

Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- 1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
- 2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- 3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- 4) Llevar a cabo un monitoreo permanente.

La Secretarí de Evaluación y Control, en su rol de Control Interno, debe asegurar que los controles sean efectivos, sean acordes al riesgo y estén funcionando en forma oportuna y efectiva.

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.

Dada la particularidad y especificidad requerida para este tipo de riesgo, se dispondrá dentro de la Matriz de Riesgos una pestaña adicional para su gestión.

6. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

6.1 Identificación de los activos de seguridad de la información

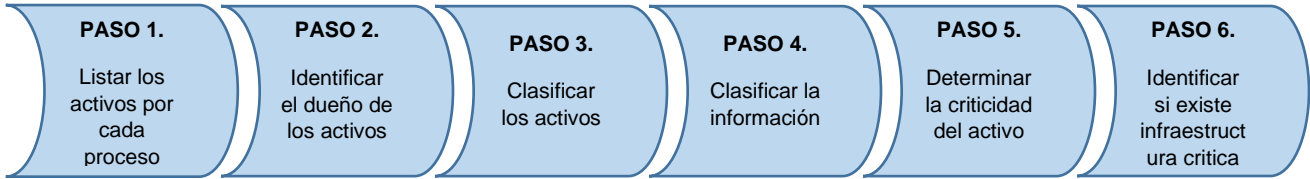
Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
<p>Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:</p> <ul style="list-style-type: none"> Aplicaciones de la organización Servicios web Redes Información física o digital Tecnologías de información TI Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital 	<p>Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).</p> <p>La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.</p>

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Identificación de activos



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas

Nota: La identificación de activos se realizará por proceso.

6.2 Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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

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

En esta actividad se genera una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia.

Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Se debe identificar las vulnerabilidades que pueden ser factores generadores de amenazas (que podrían causar daños a los activos o a la Entidad).

Indicadores clave de riesgo: hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su Sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos. En la Siguiete tabla se muestran algunos ejemplos de estos indicadores.

 Alcaldía de Itagüí	<h2 style="margin: 0;">POLÍTICA PARA LA GESTIÓN DE LOS RIESGOS</h2>
--	---

PORCESO ASOCIADO	INDICADOR	MÉTRICA
Gestión de trámites y servicios	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
Adquisiciones	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
Sistemas de información e infraestructura tecnológica	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
Talento humano	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6

Una vez identificados los “Riesgos de Seguridad de la Información”, se gestionan conforme a los lineamientos dados en este documento, para los riesgos de Gestión y el “Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas”.

7. CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción del Cambio
01	17/04/2015	Creación del documento.
02	14/03/2020	Actualización de acuerdo con la nueva guía de administración de riesgos versión 2020
03	27/12/2021	Se revisó y actualizó de acuerdo a los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de diciembre de 2020: - Actualización de definiciones: - Se incluye medición para: Apetito al riesgo, tolerancia al riesgo, Capacidad de riesgo. - Se modifica la forma como se debe describir el riesgo. -Se modifica el cuadro de clasificación del riesgo - Se modifica la valoración en la tabla de probabilidad - Se modifica la valoración en la tabla de impacto - Se modifican los mapas de Calor, Se modificó la tabla de calificación de atributos para el diseño de los controles.
04	13/03/2024	Se modificó la redacción de la parte introductoria con referencia al Modelo Integrado de Planeación y Gestión y a los requerimientos de la Guía Para la Gestión del Riesgo Vigente; Se agregaron definiciones y términos, se modificó la redacción del objetivo y la estructura del documento, incorporando los lineamientos para la gestión de los riesgos de Corrupción, Fiscales y de Seguridad de la Información.

Revisó y aprobó: Comité de Coordinación de Control Interno

ANEXO 1

LÍNEAS	RESPONSABLES	ROLES
<p>Línea Estratégica</p>	<p>Alta Dirección, Comité de Gestión y Desempeño y Comité de Coordinación de Control Interno</p>	<p>Comité de Gestión y Desempeño</p> <ol style="list-style-type: none"> Revisar el contexto estratégico, la plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el propósito de identificar cambios que puedan originar nuevos riesgos o modificar los existentes. Establecer y posicionar la Política de Administración del Riesgo de la Entidad. Revisar la información de cumplimiento de los objetivos institucionales y de los diferentes procesos, relativa a la implementación de la gestión de riesgos. Analizar el informe de evaluación a la gestión de riesgos y de ser necesario, proponer acciones para mejorar los planes para el tratamiento de los mismos. Asumir la responsabilidad primaria del Sistema de Control Interno y de la identificación y evaluación de los cambios que podrían tener un impacto Significativo en el mismo. <p>Comité de Coordinación de Control Interno</p> <ol style="list-style-type: none"> Aprobar la política de riesgos de la Entidad Evaluar y dar lineamientos técnicos sobre la administración de los riesgos de la Entidad. Retroalimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. Así mismo, hacer seguimiento a su administración, gestionar los riesgos estratégicos y aplicar los controles a los mismos. Evaluar los planes de tratamiento establecidos para cada uno de los riesgos materializados, minimizando la posibilidad de que el evento se repita.
<p>Primera Línea de Defensa</p>	<p>Secretarios de Despacho-subdirectores y Líderes de proceso</p>	<ol style="list-style-type: none"> Evaluar los cambios que se presenten en el Direccionamiento Estratégico o en el contexto estratégico, y cómo estos cambios originan nuevos riesgos o modifican los existentes. Liderar la identificación de los riesgos de los procesos a cargo, teniendo en cuenta las pautas contenidas en el procedimiento de administración de riesgos vigente. Realizar, con el apoyo de su grupo de trabajo, la administración de los riesgos identificados. Así mismo, analizar, calificar, definir controles, realizar acciones y

LÍNEAS	RESPONSABLES	ROLES
		<p>monitoreo, de acuerdo a lo establecido en la matriz de riesgos y a la periodicidad establecida, para su tratamiento y posibles mejoras.</p> <p>d. Realizar la evaluación de la solidez de los controles, para determinar la pertinencia y la necesidad de ajuste o modificación, en caso de presentarse.</p> <p>e. Adelantar la revisión, actualización periódica y seguimiento de los mapas de riesgos, en todos aquellos aspectos consignados en el procedimiento y demás directrices frente al tema, y si es el caso ajustarlo, comunicando al líder del proceso, a la coordinación de calidad y al responsable del Plan Anticorrupción y de Atención al Ciudadano – PAAC del y mapa de riesgos de corrupción si se trata de un riesgo de este tipo (Departamento Administrativo de Planeación), dichos cambios.</p> <p>f. Socializar los controles implementados, con el fin de asegurar su comprensión y oportuna aplicación, además de la información necesaria, que dé cuenta de la gestión de los riesgos. Esto se hará de forma constante en los espacios de Comités Primarios y en aquellos que se determine.</p> <p>g. Evaluar periódicamente la eficacia de los controles definidos para tratar los riesgos identificados y actualizar tales riesgos, siempre que el proceso fuente de los mismos, tenga cambios en su operatividad.</p> <p>h. Reportar los planes de tratamiento establecidos para cada uno de los riesgos materializados, incluyendo las actividades para prevenir la no repetición, así como las causas que dieron origen a la materialización de dichos eventos.</p> <p>Equipos Operativos:</p> <p>a. Apoyar el proceso de implementación de la Política Integral de Administración de Riesgos, bajo las orientaciones del Comité de Gestión y Desempeño y del Comité de Coordinación de Control Interno.</p> <p>b. Socializar y sensibilizar a los servidores de su dependencia, en la metodología para la adecuada administración de riesgos.</p> <p>c. Acompañar, programar y desarrollar con el jefe de la dependencia y/o responsable del proceso, mesas de trabajo para la revisión, identificación, análisis,</p>

LÍNEAS	RESPONSABLES	ROLES
		<p>valoración y acciones de mitigación de riesgos, con la participación de los demás servidores.</p> <p>d. Alimentar la herramienta de administración y gestión de riesgos, con la información resultante del proceso.</p> <p>De los servidores públicos y particulares que ejerzan funciones públicas en la entidad:</p> <p>a. Participar en la construcción y administración de los riesgos del proceso dentro del cual ejercen sus funciones o desarrollan sus labores.</p> <p>b. Conocer los riesgos asociados al proceso dentro del cual ejercen sus funciones o desarrollan sus labores, así como los riesgos de la Entidad, con el objeto de identificar los no previstos por los líderes de otros procesos.</p> <p>c. Identificar, registrar y reportar de manera oportuna riesgos potenciales y/o la posible materialización de un riesgo identificado, con el objeto de realizar un adecuado tratamiento y/o mitigación de los mismos.</p>
<p>Segunda Línea de Defensa</p>	<p>Departamento Administrativo de Planeación, Líderes de procesos</p>	<p>Departamento Administrativo de Planeación:</p> <p>a. Determinar la metodología para la identificación y gestión de riesgos, de acuerdo con la normatividad y los lineamientos establecidos, para cada una de las tipologías de riesgos, a excepción de aquellas tipologías de riesgos que requieren un desarrollo metodológico particular por su naturaleza, tales como: los ambientales, los de seguridad y salud en el trabajo y los de seguridad de la información.</p> <p>b. Adelantar el monitoreo del mapa de riesgos, evaluando la eficacia en la implementación de los controles y sus acciones, y visibilizando todas aquellas situaciones que dificulten o impidan la administración de los riesgos, en concordancia con la cultura del autocontrol al interior de la Entidad.</p> <p>c. Formular lineamientos que orienten a los procesos para que se desarrolle de manera eficaz, eficiente y efectiva la gestión de riesgos.</p> <p>d. Coordinar y dirigir el desarrollo de las etapas previstas para el diseño e implementación del Componente de la administración de riesgos, a través de la herramienta dispuesta para tal fin.</p> <p>e. Consolidar, solicitar y verificar la publicación del mapa de riesgos institucional.</p>



POLÍTICA PARA LA GESTIÓN DE LOS RIESGOS

LÍNEAS	RESPONSABLES	ROLES
		<p>f. Acompañar y asesorar metodológicamente a los líderes de procesos, en la administración y gestión integral de riesgos, en coordinación con la tercera línea de defensa.</p> <p>Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones - TIC: Determinar e implementar la metodología para la identificación y gestión de los riesgos de seguridad digital y los de activos de Información, de acuerdo con la normatividad y los lineamientos o parámetros establecidos, en particular, para la gestión de esta tipología de riesgos.</p> <p>Secretaría de Hacienda: Determinar e implementar la metodología para la identificación y gestión de riesgos Financieros, de acuerdo con la normatividad y los lineamientos o parámetros establecidos, en particular, para la gestión de esta tipología de riesgos.</p> <p>Secretaría de Medio Ambiente: Determinar e implementar la metodología para la identificación y gestión de riesgos ambientales, de acuerdo con la normatividad y los lineamientos o parámetros establecidos, en particular, para la gestión de esta tipología de riesgos.</p> <p>Secretaría Jurídica – Oficina de Adquisiciones:</p> <p>a. Revisar que en el estudio previo la tipificación, distribución y asignación de los riesgos previsibles, se haga dentro del marco legal y sin vulnerar derechos de las partes y terceros interesados, y que la modalidad de contratación por la que se opte sea la más conveniente y corresponda al marco de la Ley 1150 de 2007 y sus normas reglamentarias, teniendo en cuenta la justificación contenida en los estudios previos adelantados por la dependencia que necesita la adquisición del bien, servicio u obra.</p> <p>b. Verificar el comportamiento de los riesgos de cada contrato, cuando se le asigne la supervisión y/o interventoría de alguno, dando especial atención al reporte y seguimiento sobre los eventos que se monitorean, respecto a la parte que le corresponde asumir el riesgo. Cuando se trate de eventos que pudieran impactar el valor del contrato, se dará aviso</p>

LÍNEAS	RESPONSABLES	ROLES
		<p>inmediato al Ordenador del Gasto para la adopción de las medidas que correspondan.</p> <p>c. Revisar y formular los ajustes necesarios a los procedimientos y manual de riesgos de la contratación</p> <p>d. y el grupo de orientación, soporte y seguimiento de los procesos contractuales, para aplicar la Política Integral de Administración de Riesgos a todos los procesos de selección y/o contratación.</p> <p>e. Adoptar, para los riesgos relacionados con la contratación estatal, lo establecido en el Manual para la Identificación y Cobertura de riesgos en los Procesos de Contratación y/o cualquiera que al respecto se genere y /o establezca. Así mismo, los documentos CONPES que el Gobierno Nacional ha adoptado en materia de riesgos contractuales 3186 de 2002 y 3714 de 2011.</p> <p>f. Determinar e implementar la metodología para la identificación y gestión de riesgos de defensa jurídica, de acuerdo con la normatividad y los lineamientos o parámetros establecidos, en particular, para la gestión de esta tipología de riesgos.</p> <p>Secretaría de Servicios Administrativos – Oficina de Talento Humano: Determinar e implementar la metodología para la identificación y gestión de riesgos de Seguridad y Salud en el Trabajo, de acuerdo con la normatividad y los lineamientos establecidos.</p>
Tercera Línea de Defensa	Secretaría de Evaluación y Control	<p>a. Adelantar el seguimiento a los mapas de riesgos, verificando y evaluando que los líderes de los procesos desarrollen adecuadamente las etapas de identificación, valoración, seguimiento y control de los riesgos identificados, y que adelanten acciones que permitan su administración.</p> <p>b. publicar del mapa de riesgos institucional con el respectivo seguimiento en los periodos establecidos.</p> <p>c. Hacer seguimiento a la evolución de los riesgos y al cumplimiento de las acciones propuestas, con el fin de verificar su ejecución, y si es necesario proponer mejoras.</p> <p>d. Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad.</p>

LÍNEAS	RESPONSABLES	ROLES
		<ul style="list-style-type: none"> e. Evaluar la eficacia en la implementación de los controles y acciones asociadas a la administración de los riesgos. f. Acompañar y asesorar metodológicamente a los procesos, en la administración y gestión integral de riesgos, en coordinación con la segunda línea de defensa. g. Identificar y evaluar cambios que podrían tener un impacto Significativo en el Sistema de Control Interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. h. Comunicar al Comité de Evaluación y Desempeño posibles cambios evidenciados en la evaluación del riesgo, detectados durante las auditorías. i. Alertar sobre la probabilidad de riesgos de corrupción en las áreas auditadas.



POLÍTICA PARA LA GESTIÓN DE LOS RIESGOS

