Hechos para tus derechos

Personería de Itagüí

Política de Administración del Riesgo

Personería de Itagüí

2021

Centro Administrativo Municipal de Itagüí (CAMI)
Cra. 51 # 51-55 - Edificio Judicial, piso 5
Tel: 376 48 84 - info@personeriaitagui.gov.co
www.**personeriaitagui**.gov.co

ISO 9001 icontec internacional
SC - CER427866
CERTIFIED IQNet MANAGEMENT SYSTEM

Contenido

PRESENTACIÓN

La Personería de Itagüí implementó el modelo integrado de planeación y gestión MIPG, fue certificada en la Norma ISO 9001 en su versión 2015, y procede a definir su política de Administración del riesgo tomando como referente los parámetros establecidos en:

- La responsabilidad de las líneas de defensa según lo establecido en la Política de Administración de Riesgos en Función Pública en su versión 14 del 06 de julio de 2021.
- Los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5 de diciembre de 2020
- Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018
- Guía Riesgos Gestión, Corrupción y Seg.Digital DAFP – 2018
- Política de seguridad y privacidad de la información PERSONERÍA 2018

El presente documento establece los lineamientos para la identificación, análisis, valoración, evaluación y tratamiento de los riesgos que pudieran afectar la misión, el cumplimiento de los objetivos institucionales y la gestión de los procesos, programas, y planes institucionales, estos lineamientos, deben ser acatados por todos los servidores públicos de la entidad en el desarrollo de sus funciones y compromisos.

1. PLATAFORMA ESTRATÉGICA

Misión

La Personería Municipal de Itagüí es un organismo de vigilancia y control, de carácter independiente, que, en cumplimiento de sus facultades constitucionales y legales, promueve, divulga y actúa como agente de los derechos humanos, los derechos colectivos y del ambiente y garantiza la moralidad y la eficiencia administrativa, la paz y la reconciliación, a través de estrategias y acciones que permitan mejorar la función pública.

Visión

En el año 2030, la Personería Municipal de Itagüí será reconocida a nivel regional como una entidad con altos estándares de calidad, aplicando medios tecnológicos para promover y divulgar la defensa de los derechos humanos, los derechos colectivos, del ambiente y la familia, a la vez que garantiza la ética y la eficiencia administrativa, en el marco legal y del código de integridad institucional.

Política de Calidad

La Personería Municipal de Itagüí es una entidad con certificación ISO9001, que presta los servicios a sus usuarios con altos estándares de calidad, buscando un profundo nivel de satisfacción y la mejora continua en sus procesos y procedimientos, a través de la defensa y promoción de los derechos de primera, segunda y tercera generación a favor de las personas residentes y de tránsito en la ciudad de Itagüí, a su vez que promueve la eficiencia y la transparencia en la gestión administrativa de las entidades del orden central y descentralizado que manejan recursos públicos.

Código de Integridad:

- Honestidad: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con trasparencia, rectitud, y siempre favoreciendo en interés general.

- Respeto: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

- Compromiso: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

- Diligencia: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud y eficiencia para así optimizar el uso de recursos del estado.

- Justicia: Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

2. OBJETIVOS

2.1.GENERAL

Establecer los elementos y el marco general de actuación para la gestión integral de los riesgos a los que se enfrenta la Entidad y orientar las acciones necesarias que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir en el logro de su misión y objetivos institucionales y preparar la respuesta oportuna a amenazas externas que puedan generar eventos de riesgo.

2.2.ESPECÍFICOS

- Generar una visión sistémica acerca de la administración y evaluación de riesgos,

consolidando un ambiente de control adecuado a la Personería Municipal de Itagüí y un direccionamiento estratégico que fije orientación clara y planeada de la gestión, suministrando las bases para el adecuado desarrollo de la Actividad de Control.

- Reducir la vulnerabilidad y fortalecer la prevención y mitigación de los efectos de los riesgos.

- Identificar para cada proceso, además de los otros tipos de riesgos, los relacionados con la corrupción, con sus respectivas medidas para mitigar la ocurrencia de los factores internos y externos que los puedan generar.

- Involucrar y comprometer a todos los servidores de la Personería de Itagüí y a los Contratistas que apoyan la función pública, en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.

3. ALCANCE

La política de operación de riesgos es aplicable a todos los objetivos institucionales, procesos, programas, planes de la Entidad, a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones, según los riesgos establecidos y bajo la responsabilidad de las líneas de defensa.

4. GLOSARIO

Conceptos tomados de la Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5 de diciembre de 2020

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

- **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.

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

- **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.

- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **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.

- **Control:** Medida que permite reducir o mitigar 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.

- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.

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

- **Integridad:** Propiedad de exactitud y completitud.

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

- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas

- **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.

- **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.

- **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.

- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

- **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.

5. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Personería de Itagüí basada en los componentes del Modelo Integrado de Planeación y Gestión-MIPG, se compromete a ejercer el control efectivo de los posibles riesgos que puedan afectar el cumplimiento del direccionamiento estratégico de la Entidad.

5.1. IDENTIFICACIÓN DE LOS RIESGOS.

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el 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.

Se aplican las siguientes fases:

Análisis de objetivos institucionales y de procesos: Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo institucional o del proceso.

Análisis de objetivos estratégicos	Análisis de los objetivos de proceso
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso. Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).	Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos. A continuación encontrará un ejemplo de análisis en el proceso de contratación: La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continua operación.

Fuente: Comitte of Sponsoring Orgizations of the Treadway Commission COSO Marco Integrado. Componente Evaluación de Riesgos, Principio. p. 73. 2013.

S ***Specific*** **(específico):** Lo importante es resolver cuestiones como: qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.

M ***Mensurable*** **(medible):** Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas (cuando aplique).

A ***Achievable*** **(alcanzable):** Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o cómo resultaría mejor.

R ***Relevant*** **(relevante):** Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación.

T ***Timely*** **(temporal):** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

- **Identificación de los puntos de riesgo:** son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

- **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. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

- **Identificación de áreas de factores de riesgo:** son las fuentes generadoras de riesgos.

5.1.1. Identificación de riesgos operativos.

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los objetivos institucionales.

Las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo institucional o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto.

¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo con el desarrollo del proceso.

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo.

5.1.2. Identificación de riesgos de corrupción.

Definición de 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 concurran los **componentes de su definición**, así:
ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

5.1.3. Identificación de riesgos de seguridad digital.

Como lo indica el **Paso 2** 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, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- 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. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Identificación de Amenazas:

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

- Deliberadas (D)

- Fortuito (F)
- Ambientales (A).

5.2.RESPONSABILIDADES SOBRE LA IDENTIFICACIÓN DE RIESGOS

5.2.1. Planeación Institucional.

De igual manera, el líder de Planeación Institucional llevará a cabo las siguientes acciones durante el acompañamiento para la identificación del riesgo:

- Socializar la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo, comunicación de los planes y programas del proceso.

- Capacitar al grupo de trabajo de cada dependencia en la herramienta SGC para la gestión del riesgo.

- Liderar las mesas de trabajo de identificación del riesgo.

- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología.

- Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en el SGC.

- Elaborar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los equipos de trabajo. Presentar la propuesta para aprobación.

- Una vez aprobado, comunicar al líder del proceso los resultados de las mesas de identificación de trabajo y recordar la importancia de socializarlos al interior de su dependencia.

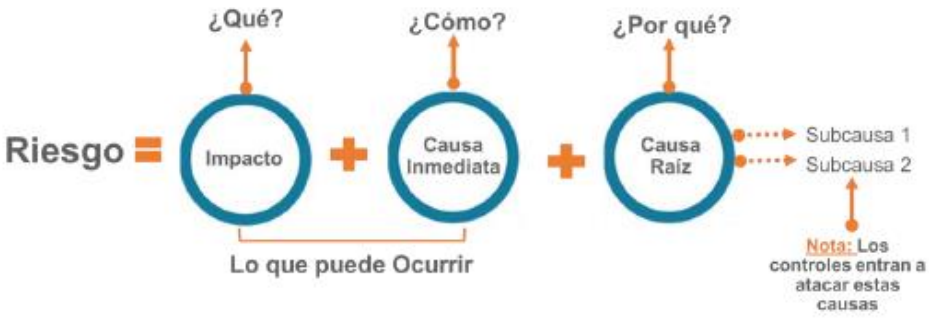
- Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso, con los riesgos altos, extremos y de corrupción.

5.2.2. Líder de la Delegatura u oficina

Asegurar, que al interior de su grupo de trabajo se reconozca el concepto de "administración del riesgo", la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa. El líder se encargará de la identificación, monitoreo, seguimiento trimestral, reporte y socialización del riesgo asociados.

5.3.DESCRIPCIÓN DEL RIESGO

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



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

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

Desglosando la estructura propuesta tenemos:

- 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.

Premisas para una adecuada redacción del riesgo

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

5.4.CLASIFICACIÓN DE LOS RIESGOS

5.4.1. Tipos de Riesgos.

Con el fin de mantener una terminología común para las actividades de gestión de riesgos, la Entidad establece la siguiente clasificación de riesgos:

- Calidad: Relacionados con los atributos de calidad establecidos en MIPG, las políticas de aseguramiento y control de calidad.
- Contractual: Relacionado con los atrasos o incumplimientos de las etapas contractuales en cada vigencia
- Comunicación: Relacionado con los canales, medios y oportunidades para informar durante las diferentes etapas de un programa, un plan, un proceso o la gestión institucional
- Cumplimiento y conformidad: Se asocian con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad

- Estratégicos: Asociado a la administración de la Entidad, a la misión y el cumplimiento de los objetivos institucionales, la definición de políticas, y el diseño de lineamientos que respondan a las necesidades de las partes interesadas de la Entidad.
- Financieros: Relacionado con la ejecución presupuestal y el manejo de los bienes
- Imagen: Relacionado con la percepción y la confianza por parte de las partes interesadas frente a la Entidad
- Operativos: Riesgos provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias
- Tecnológicos: Relacionados con la capacidad tecnológica (Hardware, Software, Redes) para satisfacer sus necesidades actuales, futuras y el cumplimiento de la misión.
- Digitales: Son los relacionados con el daño en los medios digitales como el ciber ataque, los virus entre otros.
- Corrupción: Se entiende por Riesgo de Corrupción la posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de la entidad y del Estado, para la obtención de un beneficio particular.

5.4.2. Riesgo Inherente.

Es aquel que se puede presentar o es relacionado con que hacer diario institucional. Puede ser generado por causas internas o externas y afectar la estabilidad y el desarrollo de la gestión de la personería. No puede ser eliminado, por lo cual su identificación debe contemplarse en el mapa de riesgos institucional.

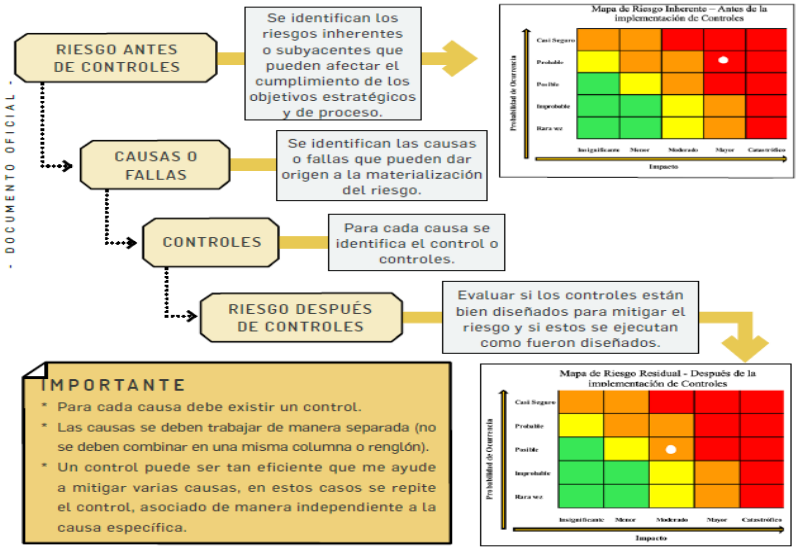
5.4.3. Riesgo Residual.

Nivel de riesgo (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 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.

La identificación del riesgo inherente y del riesgo residual se muestra en la siguiente imagen:



5.5.GESTIÓN DEL RIESGO

5.5.1. Metodología para la gestión del riesgo.

La Personería Municipal de Itagüí, cuenta con el sistema de gestión de la calidad (SGC) en el cual registra seguimientos a los riesgos según la periodicidad establecida en el mapa de riesgos institucional.

El seguimiento de los riesgos de proceso es responsabilidad de cada líder y se realiza de forma trimestral, cuatrimestral, semestral o anual.

El seguimiento de los riesgos de corrupción, es de forma cuatrimestral y es responsabilidad del jefe de la oficina de control interno.

Estos seguimientos se remiten al servidor responsable de actualizar el Sistema de gestión de la calidad (SGC), el periodo establecido para la entrega de estos seguimientos son los 10 días hábiles siguientes al finalizar la fecha de corte (Trimestral, cuatrimestral entre otros)

Por lo menos una vez al año se revisará el mapa de riesgos institucional y se harán los ajustes o actualizaciones necesarios según los requerimientos del Departamento Administrativo de la Función Pública (DAFP).

5.5.2. Definición de los controles.

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

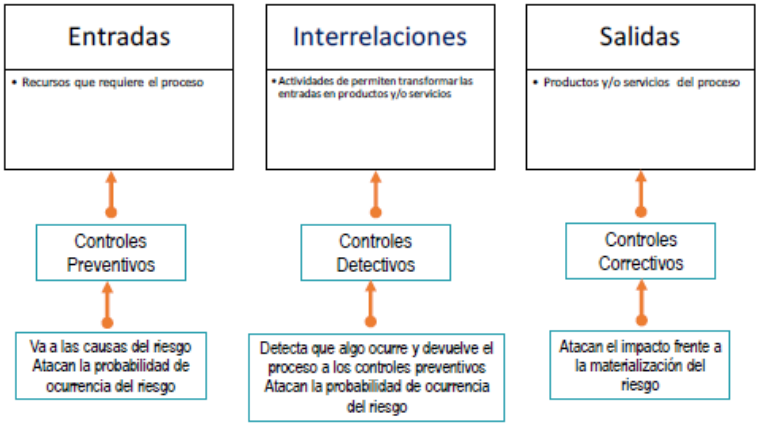
- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo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

Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

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

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

comprender esta estructura conceptual, en la siguiente figura se consideran 3 fases globales del ciclo de un proceso así:



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

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

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 – Atributos: A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y

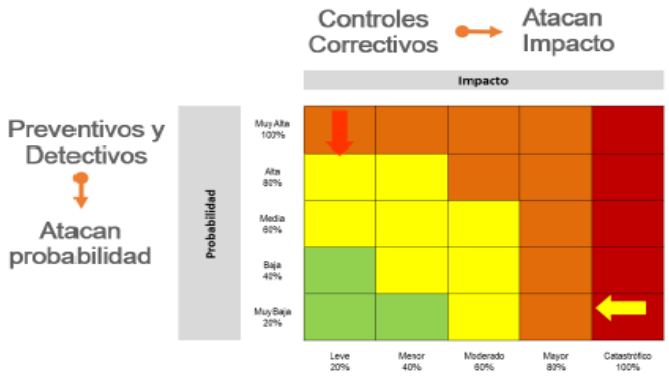
la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

Características			Descripción	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	25%

Características			Descripción	Peso
			intervención de personas para su realización.	
		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.	-

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

***Nota:** Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

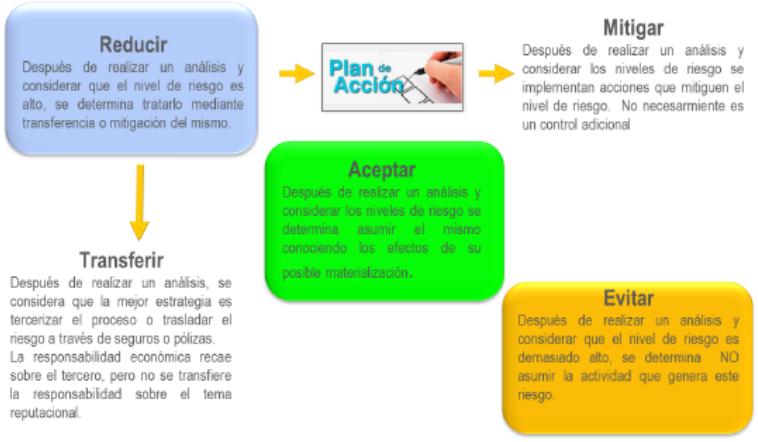


Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

5.5.3. Estrategias para combatir el riesgo.

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

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



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

5.5.4. Niveles de aceptación del riesgo.

Acorde con los riesgos residuales presentados por los líderes de procesos y aprobados en el comité institucional de gestión y desempeño, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

Se determina que para los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo baja, está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

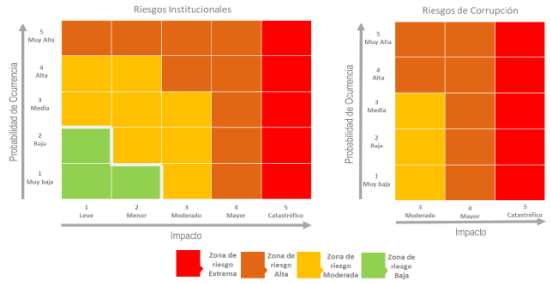
5.5.5. Niveles para calificar el impacto.

Tabla 5 Criterios para definir el nivel de impacto

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

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

Gráfica 1. Matriz de calificación de nivel de severidad del riesgo



5.5.6. Tratamiento de riesgos.

5.5.6.1. **Tratamiento de los riesgos Operativos y de corrupción**

De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

Gestión de eventos: un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Petición al contratista (Ingeniero) apoyo de sistemas.
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Abogados.

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

Desempeño del control= # eventos / frecuencia del riesgo (# veces que se hace la actividad)

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.

5.5.6.2. Tratamiento de los 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.

- En la Personería Municipal de Itagüí, la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información en la entidad.
- Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.
- Se deben identificar los riesgos a los que se encuentran expuestos los activos de información de la entidad.
- Los riesgos de seguridad de la información analizados deben ser objeto de tratamiento (mitigar, transferir, evitar, aceptar), dicho tratamiento debe ser coherente con los criterios de aceptación de riesgos.
- Los riesgos deben ser monitoreados después de su tratamiento para asegurar que siguen estando en niveles aceptables para la entidad.
- En los casos que se realice la estimación económica de los riesgos, se debe asegurar que el valor de la aplicación de medidas de mitigación sea inferior al costo de las consecuencias de la materialización de los riesgos
- En la Personería Municipal de Itagüí los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.
- Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia (confirmada o sospechada) de situaciones que afecten la seguridad de la información.
- Debe conformarse y mantenerse un equipo multidisciplinario para la respuesta y tratamiento a los incidentes de seguridad de la información.
- La atención de incidentes debe seguir el procedimiento descrito en el sistema de gestión de la calidad Gestión de Peticiones de Servicios e Incidentes.

5.5.7. Niveles de responsabilidad en el manejo del riesgo

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité Institucional de Gestión y Desempeño	• Analizar los riesgos, vulnerabilidades y amenazas institucionales para el cumplimiento de los objetivos, planes, metas y compromisos de la entidad. • Definir el marco general para la gestión del riesgo, la gestión de la continuidad y el control. • Recomendaciones para la política de operación para la administración del riesgo.
	Comité Institucional de Coordinación de Control Interno.	• Someter a aprobación del Personero la política de administración del riesgo previamente estructurada por parte del Área de Planeación, como segunda línea de defensa en la entidad. • Definir y aprobar el marco general para la gestión del riesgo y el control incluidos en la política de riesgo. • Revisar la política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional.
Primera Línea	Líderes de Proceso	• Asegurar que al interior de su grupo de trabajo se conozca la política de

		administración de riesgo aprobada por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. • Delegar, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos. • Realizar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y su documentación se evidencie en los procedimientos de los procesos. • Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. • Informar al líder del proceso de Planeación (segunda línea) sobre los riesgosmaterializadosenlosobjetivos, programas y planes de los procesos acargo. • Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación.

		• Comunicar al equipo de trabajo los resultados de la gestión del riesgo.
	Servidor delegado para el manejo de riesgos en cada proceso	• Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento. • Revisar y actualizar el mapa de riesgos con el acompañamiento del asesor (a) del SGC. • Realizar la medición y análisis a la gestión efectiva de los riesgos. • Reportar en el SGC- Sistema de Gestión de la Calidad los seguimientos, avances, y evidencias de la gestión de los riesgos dentro de • los plazos establecidos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • En caso de la materialización de un riesgo no identificado, este debe ser incluido en el mapa de riesgos institucional. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces.
	Servidores en General	• Estar en vigilancia y control del quehacer diario de la dependencia, donde se verifica

		la efectiva gestión de los riesgos establecidos. • Analizar e informar en la gestión del día a día si se materializó algún riesgo de los que se encuentran establecidos en el mapa de riesgos institucional.
Segunda Línea	Líder del proceso de Planeación Institucional (En la Personería Municipal de Itagüí, el proceso de Planeación es liderado por el Personero)	• Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. • Revisar que el cargue de información en el SGC esté acorde con lo aprobado y remitido por cada líder del proceso. • Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. • Comunicar a los líderes de proceso a través de los enlaces los resultados de la gestión del riesgo.

		• Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso). • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. • Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser incluido en el mapa de riesgo institucional. • 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 impacto de los riesgos.

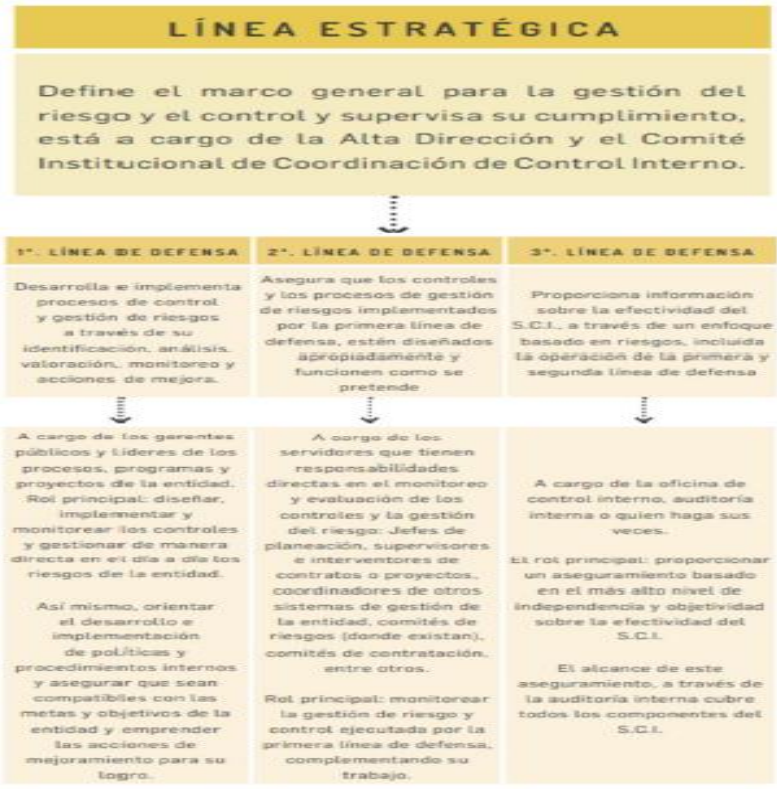
		• Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos en el CICCI. • Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad. • Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Consolidar el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Gestión y Desempeño. • Presentar al CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos

		identificados en las áreas en los diferentes niveles de operación de la entidad. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Orientar a la primera línea de defensa para definir la estrategia de continuidad del negocio identificando los escenarios.
Segunda Línea	Secretaria General, Como líder del proceso de Gestión de bienes y servicios (Gestión de contratos), Atención al Ciudadano, Gestión Documental, y Talento Humano.	• Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo y la definición de controles en los temas a su cargo. Incluyendo el enfoque en la prevención del daño antijurídico • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Realizar el seguimiento al mapa de riesgos de su proceso. • Reportar en el módulo de riesgos del SGC o delegar a un profesional de la dependencia a su cargo, el registro de los avances en la gestión del riesgo. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo.

		• Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
Tercera Línea	Oficina de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Proporcionar aseguramiento objetivo, en las áreas identificadas no cubiertas por la segunda línea dedefensa. • Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño decontroles. • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos (De proceso y de corrupción) de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. • Recomendar mejoras a la política para la administración del riesgo. • Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

5.6.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 como se muestra en la siguiente tabla.



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

5.7. ACTUALIZACIÓN POLÍTICA

La política de Administración del Riesgo de la Personería de Itagüí, se revisará cada vigencia y se analizará según los parámetros establecidos por el Departamento Administrativo de la Función Pública-DAFP si es necesaria su actualización.

Planeación Institucional
2021