RESOLUCIÓN No. 013 DE 2024
(01 DE ABRIL DE 2024)

"POR LA CUAL SE ADOPTA LA POLÍTICA INSTITUCIONAL PARA LA ADMINISTRACIÓN DEL RIESGO DEL FONDO MIXTO PARA EL DESARROLLO INTEGRAL Y LA GESTIÓN SOCIAL DE COLOMBIA FONCOLOMBIA"

El Director ejecutivo del **FONDO MIXTO PARA EL DESARROLLO INTEGRAL Y LA GESTIÓN SOCIAL DE COLOMBIA-FONCOLOMBIA** en uso de sus facultades legales y en especial las conferidas en especial las que le confiere el artículo 2.2.22.3.8 del Decreto 1083 de 2015 y demás normas concordantes y

CONSIDERANDO:

Que la Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado, en el literal f del Artículo 2 establece como uno de los objetivos del Sistema de Control interno: *"definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos".*

Que en la Ley 1474 de 2011, se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Que la Política de Administración del Riesgo, fija los lineamientos y las guías de acción para el control y mitigación de los riesgos.

Que el modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo.

Que el Decreto 1499 de 2017, en su artículo 2.2.22.3.2 define el Modelo integrado de Planeación y Gestión (MIPG) como "... un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos.

Que se hace necesario adoptar en la entidad la Política de Administración del Riesgo con el fin de que opere como lineamiento para el tratamiento, manejo y seguimiento a los riesgos que puedan afectar el cumplimiento de los objetivos de la entidad.

En mérito de lo expuesto,

RESUELVE:

ARTICULO PRIMERO: ADOPTAR. la Política de Administración del Riesgo para el **FONDO MIXTO PARA EL DESARROLLO INTEGRAL Y LA GETIÓN SOCIAL DE COLOMBIA-FONCOLOMBIA**, la cual hace parte integral de la presente resolución.

ARTICULO SEGUNDO. ACTUALIZACIÓN: La política de Administración del Riesgo, se actualizará conforme a los lineamientos normativos impartidos por el Departamento Administrativo de la Función Pública.

ARTICULO TERCERO. VIGENCIA: La presente resolución rige a partir de la fecha de su expedición.

Dado en Bucaramanga, Santander al primer (1) día del mes de abril de 2024.

PUBLÍQUESE Y CÚMPLASE

JHON JAIRO MENESES QUINTERO
DIRECTOR EJECUTIVO
FONCOLOMBIA

Proyectó: Yody Andrea Santamaría Quiroga
Jefe Oficina de Planeación

Revisó: Viviany González Gamarra
Jefe Oficina de Control Interno

El FONDO MIXTO PARA EL DESARROLLO INTEGRAL Y LA GESTIÓN SOCIAL DE COLOMBIA-FONCOLOMBIA se compromete a identificar, evaluar, controlar, prevenir y mitigar los riesgos que puedan afectar el desarrollo de los procesos, los objetivos institucionales, planes, proyectos, determinando y aplicando las acciones de control preventivas para evitar la materialización de los riesgos.

OBJETIVO DE LA POLITICA

Establecer los lineamientos para la correcta identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales en el marco de los procesos, planes y proyectos de la entidad, así como orientar en las acciones preventivas que conduzcan a disminuir la materialización de los riesgos.

OBJETIVOS ESPECIFÍCOS

- Adoptar una metodología que permita a FONCOLOMBIA gestionar de manera efectiva los riesgos que afectan el logro de los objetivos institucionales.
- Identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades para la gestión de los riesgos.
- Reducir la posibilidad de materialización de los riesgos en cada proceso, definiendo actividades de control encaminadas a fomentar la transparencia en la gestión.
- Fortalecer la cultura de control de la entidad.
- Orientar a la toma de decisiones oportuna, con el fin de dar continuidad a la gestión institucional.

ALCANCE

La política de administración del riesgo aplica a todos los procesos, planes y proyectos de la entidad, bajo la responsabilidad de quienes ejecuten labores en cada uno de los procesos.

GLOSARIO[1]

- **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.

- **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.

- **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.

- **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.

- **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.

[1] Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 -2022

- **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.

RESPONSABILIDAD

Responsabilidad frente a los riesgos conforme al esquema de líneas de defensa:

LINEA ESTRATEGICA La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad.	**RESPONSABLES** Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno.
• Definir y aprobar la Política de Administración del Riesgo, la evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes.	
PRIMERA LINEA DE DEFENSA Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos.	**RESPONSABLES** Jefes o Líderes o de cada una de las áreas.
• Corresponde la identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.	
SEGUNDA LINEA DE DEFENSA Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.	**RESPONSABLES** Jefe oficina de planeación e infraestructura, jefe oficina jurídica, jefe oficina financiera, jefe oficina talento humano, coordinadores.
• Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de	

prácticas de gestión de riesgo eficaces. • Consolidar y analizar la información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.	
TERCERA LINEA DE DEFENSA Evalúa independiente la efectividad del sistema de gestión de riesgos.	**RESPONSABLES** Jefe de control interno o quien haga sus veces
• Asesorar, orientar técnicamente y realizar las recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces. • Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. • Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. • Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.	

LINEAMIENTOS PARA LA GESTIÓN DEL RIESGO

1. Identificación del riesgo

Tiene como objetivo identificar los riesgos que estén o no bajo el control de la entidad, para ello se debe tener en cuenta el contexto estratégico en el que opera la 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 estratégicos y de los procesos:** Todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.
- **Identificación de los puntos de riesgo:** 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 se 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 entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.
- **Identificación áreas de factores de riesgo:** Corresponden a las fuentes generadoras de riesgos que puede tener la entidad, como se muestra a continuación:

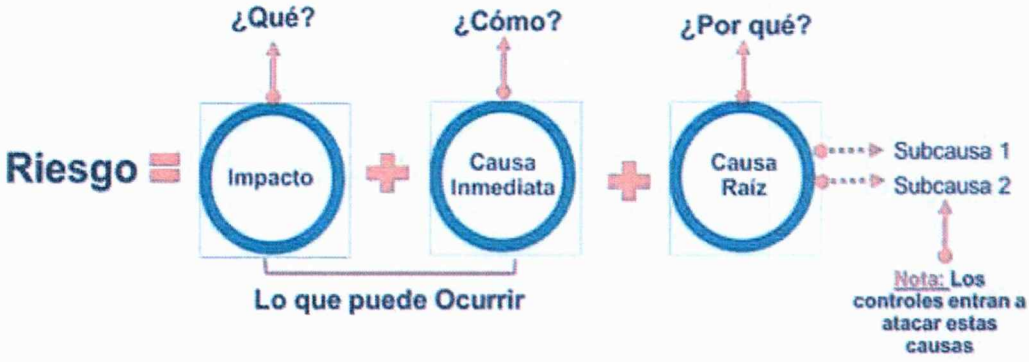
Factor	Definición	Descripción

Procesos	Eventos relacionados con errores en las actividades que deben realizar los trabajadores en la entidad	Falta de procedimientos
		Errores autorización
		Errores de cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción	Hurto activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público, fenómenos naturales.

2. Descripción del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender, de acuerdo a la guía de administración del riesgo, la estructura detallada a continuación facilita la redacción y claridad del riesgo iniciando con la frase POSIBILIDAD DE con los siguientes aspectos:

Figura 10 Estructura propuesta para la redacción del riesgo



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6 – 2022*

Impacto: Las consecuencias que puede ocasionar a la organización la materialización de 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.

3. CLASIFICACIÓN DE LOS RIESGOS

La clasificación del riesgo permite agrupar los riesgos identificados, identificándose en las siguientes categorías:

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6 - 2022*

4. VALORACIÓN DEL RIESGO

La valoración del riesgo establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo (riesgo inherente)

4.1 ANÁLISIS DE RIESGOS

El análisis de riesgos, busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto:

Determinar la Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo.

Los criterios para medir el nivel de la probabilidad se definen de la siguiente manera:

Criterios para definir el nivel de probabilidad

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

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6 2022*

Determinar el Impacto: Se entiende por impacto, las consecuencias que puede ocasionar a la entidad la materialización del riesgo. El impacto se puede clasificar en impacto económico y reputacional.

Es importante tener en cuenta que cuando se presenten ambos impactos para un riesgo tanto económico como reputacional, se debe tomar el nivel más alto.

Los criterios para definir el nivel de impacto es el siguiente:

Criterios para definir el nivel de impacto

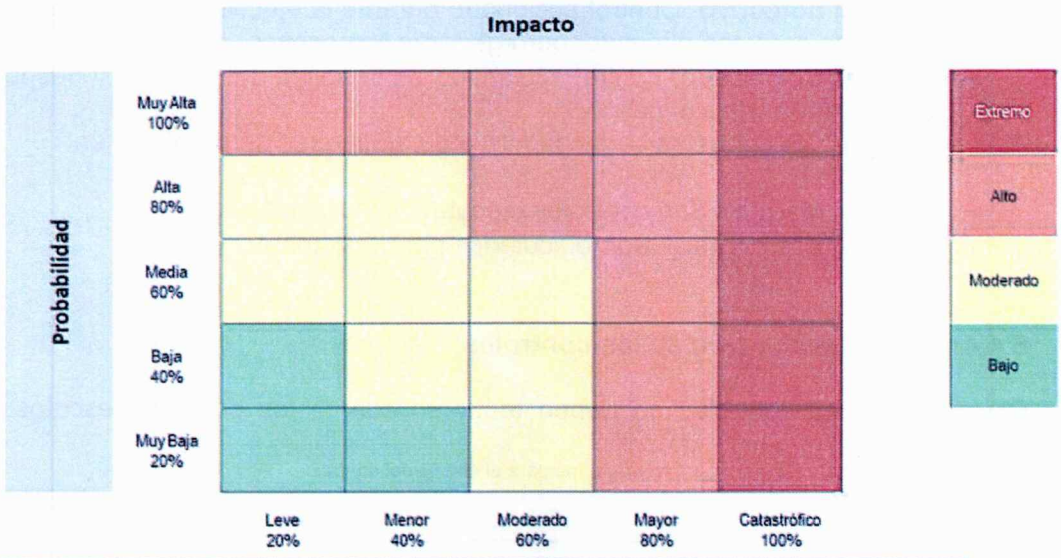
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
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: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 – 2020*

5. EVALUACION DE RIESGOS

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

Matriz de calor (niveles de severidad del riesgo)



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6 – 2022*

5.1 Valoración de controles:

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

5.2 Estructura para la descripción del control:

- **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.

5.3 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.

Adicionalmente, los controles según la forma de ejecutarse se clasifican en:

- **Control Manual:** Son controles ejecutados por personas.
- **Control Automático**: Son ejecutados por un sistema.

5.4 Análisis y evaluación de los controles:

Para evaluar los controles se deben tener en cuenta los criterios descritos en la siguiente tabla:

Atributos 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%

Caracteristicas			Descripción	Peso
		Manual	Controles que son ejecutados por una persona, tiene implicito 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: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6 – 2022*

6. ESTRATEGIAS PARA COMBATIR EL RIESGO

Corresponde a la decisión que se toma frente al riesgo, esta puede ser aceptar, reducir o evitar.

Estrategias para combatir el riesgo

Reducir	Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
Mitigar	Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.
Aceptar	Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
Transferir	Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
Evitar	Después de realizar un análisis y considerar que el nivel del riesgo es demasiad alto, se determina NO asumir la actividad que genera este riesgo.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6– 2022*

7. MONITOREO Y REVISIÓN

El modelo integrado de planeación y gestión MIPG, desarrolla en la dimensión 7 el Modelo Estándar de Control Interno MECI y las líneas de defensa como eje articulador para identificar la responsabilidad de la gestión de riesgo y control.

8. LINEAMIENTOS PARA EL ANÁLISIS DE RIESGO FISCAL

8.1 Control fiscal interno y prevención del riesgo fiscal

El control fiscal interno tiene como finalidad prevenir los elementos constitutivos de la responsabilidad fiscal, que es el daño al patrimonio público, representado en el menoscabo, disminución, perjuicio, pérdida o deterioro de los bienes o recursos públicos o a los intereses patrimoniales del Estado (Decreto 403 de 2020, art.6).

El control fiscal interno es el primer nivel de vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El control fiscal interno hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes e intereses patrimoniales de naturaleza pública y de las líneas de defensa en lo que corresponde a cada una de ellas.

El control interno potencia el enfoque preventivo, partiendo que el Sistema de control Interno es fundamental para el logro de resultados, con la prevención de riesgos de gestión, corrupción, y fiscales así como con la seguridad del gestor público (jefes de la entidad, ordenadores del gasto y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de las labores de cobro, entre otros), a través de la prevención de responsabilidades.

8.2 Definición y elemento del riesgo fiscal

El riesgo fiscal se define como "Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial".

Elementos que componen el riesgo fiscal

Efecto: Daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, referidos a riesgos fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.

8.3 Metodología para el Levantamiento del mapa de riesgo fiscales

Una adecuada identificación, clasificación, valoración y control del riesgo fiscal, es fundamental para el resultado de la gestión de la entidad y para la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros).

- **Identificación de riesgos fiscales:** Para identificar los riesgos fiscales es necesario que se establezcan los puntos de riesgo fiscal y las circunstancias inmediatas.
  Los puntos de riesgo fiscal son todas las actividades que representan gestión fiscal, igualmente se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales, y/o fallos con responsabilidad fiscal.

- **Identificación del área de impacto:** El área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la entidad en caso de materializarse el riesgo.

- **Descripción del riesgo fiscal:** Para la descripción del riesgo fiscal se debe tener en cuenta:

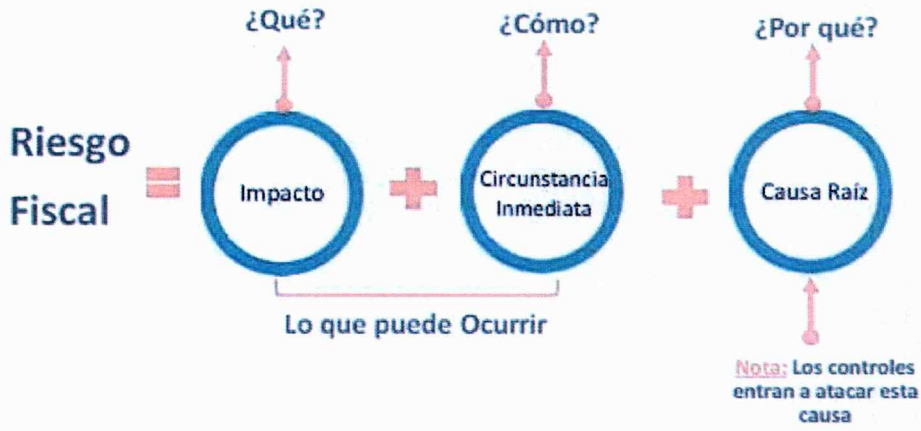
  - Iniciar con la oración: Posibilidad de, debido a que se esta refiriendo al evento potencial.

  - Impacto: Corresponde al que. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

  - Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica-causa raíz- para que se presente el riesgo.

  - Causa raíz: Corresponde al porqué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada.

Estructura para la redacción de riesgos fiscales



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6– 2022*

- **Valoración de riesgo fiscal**

  Evaluación de riesgos: Busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

  Probabilidad: Es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

  Impacto: Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.
  Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales,

- **Valoración de controles:** Con el fin de propiciar el logro de los objetivos, las actividades de control se orientan en prevenir y detectar la materialización de los riesgos.

  Tipologías de controles:

- Control Preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de

riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.

- Control detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- Control Correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.

9. RIESGO DE CORRUPCIÓN

El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Los riesgos de corrupción deben tener en cuenta los siguientes criterios:

- Se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Generalidades acerca de los riesgos de corrupción

- Se deben elaborar anualmente por cada responsable de los procesos al interior de la entidad.

- Después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción. Se debe dejar por escrito las modificaciones o inclusiones realizadas.

- **Consolidación**: La oficina de planeación o quien haga sus veces le corresponde liderar el proceso de administración del riesgo, igualmente le corresponde consolidar el mapa de riesgos de corrupción.

- **Publicación del mapa de riesgos de corrupción:** Se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

- **Monitoreo:** En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

- **Seguimiento:** El jefe de control interno o quien haga sus veces, realizará seguimiento a la gestión de los riesgos de corrupción. En este sentido es necesario que en los procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

  Primer seguimiento: Con corte al 30 de abril, la publicación deberá realizarse dentro de los diez (10) primeros días del mes de mayo.

  Segundo seguimiento: Con corte al 31 de agosto, la publicación deberá realizarse dentro de los diez (10) primeros días del mes de septiembre.

  Tercer seguimiento: Con corte al 31 de diciembre, la publicación deberá realizarse dentro de los diez (10) primeros días del mes de enero.

  El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad.

9.1 IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN

Los riesgos de corrupción siempre deben gestionarse e igualmente, en la descripción de los riesgos de corrupción deben concurrir TODOS los componentes para su definición:

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

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6– 2022*

9.2 VALORACION DEL RIESGO DE CORRUPCIÓN

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Los siguientes criterios se deben tener en cuenta en la valoración del riesgo de corrupción para calificar la probabilidad:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6–2022*

9.3 ANÁLISIS DEL IMPACTO PARA LOS RIESGOS DE CORRUPCIÓN

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

10. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

- **Identificación de los activos de seguridad de la información:** Para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

  Activos de Información: Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización

  Los activos de información permiten determinar qué es lo más importante que la entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

  Los activos pueden ser:
- Servicios web
- Redes
- Información física o digital
- Tecnología de Información TI

- Tecnologías de operación TO que utiliza la entidad para funcionar en el entorno digital.

Identificación del riesgo de seguridad de la Información:

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

- **Valoración del Riesgo de seguridad de la Información:** Se asociarán las tablas de probabilidad e impacto definidas en el ítem 4.1 Análisis de Riesgos.

- **Controles asociados a la seguridad de la Información:**

Se podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.

BIBLIOGRAFIA

Guía para la administración del riesgo y el diseño de controles en entidades públicas, Dirección de Gestión y Desempeño Institucional Versión 6 noviembre de 2022

Manual Operativo del Modelo Integrado de Planeación y Gestión Consejo para la Gestión y Desempeño Institucional Versión 5 marzo de 2023.