FONDECUN

FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

CUNDINAMARCA ¡REGIÓN Que Progresa!

Gobernación de Cundinamarca

Sede Administrativa
Av. Carrera 10 No. 28-49 Torre A, Piso 21
Teléfonos: 243 2328 / 243 2806

www.fondecun.gov.co
@fondecun

CONTENIDO

1. INTRODUCCIÓN

El logro de los objetivos al interior de las organizaciones es enfrentar diferentes factores e influencias internas y externas, que crean incertidumbre sobre su cumplimiento, este efecto se conoce como el riesgo.

Es por eso que el Interior del Fondo de Desarrollo de Proyectos de Cundinamarca, se ha decidido implementar una Política de Administración del Riesgo, que permita gestionar el riesgo presente en el logro de sus objetivos estratégicos, mediante su identificación y análisis, evaluando y controlando los riesgos, por medio de acciones a través de planes que minimicen los efectos no deseados (tratamiento del riesgo).

A través de esta Política, se establecerán los principios necesarios para hacer que la administración y gestión del riesgo sea eficaz, eficiente y coherente, siendo necesario que se implemente en todos los niveles del fondo, así como en los proyectos y actividades que desarrolla, teniendo siempre en cuenta su contexto, su entorno, sus partes involucradas y la diversidad de criterios de riesgos.

por esa razón, y teniendo en cuenta el modelo integrado de planeación y gestión, MIPG, que integra los sistemas de gestión de la calidad y de desarrollo administrativo; se crea un único sistema de gestión articulado con el Sistema de Control Interno, el Fondo de Desarrollo de Proyectos de Cundinamarca define su política del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión en los procesos, así como los del Modelo Estándar de Control Interno, en lo referente a las líneas de defensa, los lineamientos de la Guía para la administración del riesgo Versión 5 de la Función Pública, la cual articula los riesgos de gestión, corrupción y de seguridad digital y la estructura del Sistema Integrado de Gestión — SGI en el módulo de riesgos.

2. OBJETIVO

Valorar y tratar los riesgos de gestión, seguridad digital, de corrupción y los que puedan presentarse con respecto a la eventual implementación de sistemas de gestión adicionales en la organización.

2.1 Objetivos específicos

i. Identificar los riesgos para los tipos de objetivos estratégicos, apoyo y misionales del Fondo

ii. Identificar los riesgos de corrupción del Fondo.

iii. Identificar los riesgos de seguridad de la información o de seguridad digital para el Fondo.

iv. Integrar la gestión de riesgo en los procesos organizaciones, a través del diseño, documentación, establecimiento, implementación y mejora continua de controles.

v. Actuación correctiva y oportuna frente la materialización de riesgo

Para el desarrollo de estos objetivos se definirán acciones dentro del plan de acción anual de la entidad, a cargo de las distintas funciones, niveles y procesos de la organización.

3. ALCANCE

La política contenida en este documento es aplicable a los objetivos estratégicos, tácticos y operativos, de los sistemas de gestión implementados en la entidad y a todos los procesos de la organización. El alcance de la política no tiene una delimitación temporal.

Esta política no es aplicable a la "Identificación de Peligros, Evaluación y Valoración de los Riesgos", de que trata el Decreto 1072 de 2015 sobre el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) o las normas internacionales que pudieran ser aplicadas como marco de referencia para la implementación de un SG-SST. Para ello, se definirán los criterios para la identificación de peligros, y la evaluación y valoración de los riesgos, según sea definido en las reglamentaciones, regulaciones y guías técnicas colombianas aplicables.

4. 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.

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

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

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.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

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.

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.

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.

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5

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

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.

Contingencia: Posible evento futuro, condición o eventualidad.

Crisis: Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

Mapa de Riesgos: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.

Restablecimiento: Capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.

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

5. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos del Fondo de Desarrollo de Proyectos de Cundinamarca, genera un entorno permanente de lucha y cero tolerancias contra la corrupción, integrando sus procesos enfocados a la prevención y detección de hechos asociados a este fenómeno, tomando las medidas necesarias para combatirlo mediante la política de riesgos y cuenta con un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión, la guía de administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los funcionarios de la entidad y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

La presente política involucra a todos los Servidores Públicos del Fondo de Desarrollo de Proyectos de Cundinamarca, a todos los procesos, procedimientos que integran los procesos, quienes establecen los lineamientos que permitan la identificación, el análisis, la valoración, el tratamiento y el seguimiento de las acciones con el fin de mitigar los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales y, para lo cual la oficina asesora de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento, cargue de información y dispone un manual de uso para el servicio de todos los procesos.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso

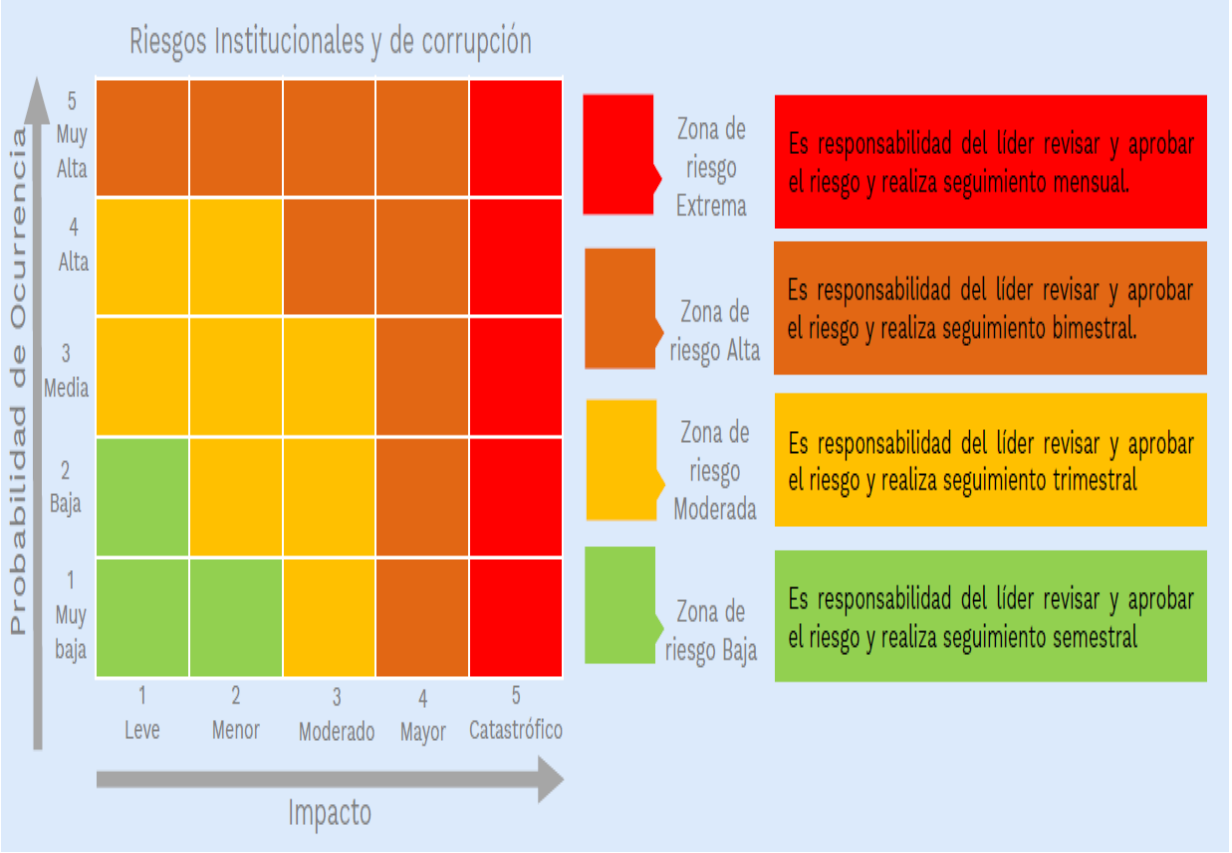
6. NIVELES DE ACEPTACIÓN O TOLERANCIA AL RIESGO[2]

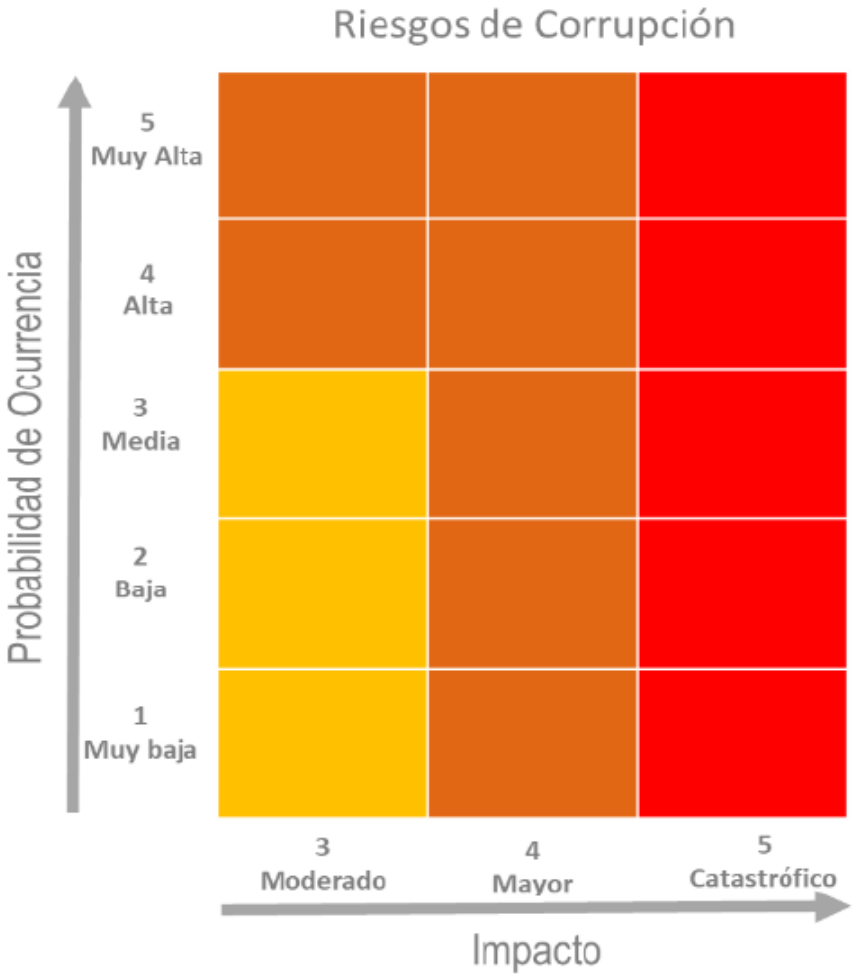
Para riesgos de gestión y de seguridad digital, se consideran aceptables o tolerables los que se ubiquen en zonas de riesgo inherente o residual baja; para los cuales es optativo la definición de acciones para el tratamiento o abordaje de riesgos.

Son inaceptables o intolerables los riesgos de corrupción en cualquier zona de riesgo inherente o residual.

[2] Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5

Matriz de calificación de nivel de severidad del riesgo





7. RESPONSABILIDADES

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 de Gestión y Desempeño	• Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. • Definir el marco general para la gestión del riesgo, la

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
	Institucional	gestión de la continuidad del negocio y el control. • Recomendaciones de mejoras a la política de operación para la administración del riesgo.
	Comité institucional de coordinación de control interno	• Aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico, previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización y evaluar su eficacia. • 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. se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios.
Primera Línea	Líderes de proceso	• Asegurar que al interior de su grupo de trabajo se reconozca el concepto de "Administración de Riesgo" la política, metodología y marco de referencia de Fondecun. • Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera con énfasis en la prevención del daño antijurídico. • Delegar, por parte del líder del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. • Revisar el adecuado diseño de los y ejecución de los controles establecidos para mitigación de los riesgos y determinar las acciones de mejora a que haya lugar. • Desarrollar ejercicios de autoevaluación para establecer la

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		eficiencia, eficacia y efectividad de los controles. • Informar a planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. • Reportar a Planeación los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. • En caso de la materialización de un riesgo no identificado, este debe ser informado a Planeación y ser incluido en el mapa de riesgo institucional.
Segunda Línea	Planeación	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Capacitar al grupo de trabajo de cada dependencia en la la gestión del riesgo con la asesoría del Jefe de control interno. • Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos. • 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 de Gestión y Desempeño Institucional • Presentar al Comité Institucional de Coordinación de Control Interno 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. • Socializar y publicar el mapa de riesgos institucional. • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados • Revisar el adecuado diseño de los controles para la

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		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. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología • 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. • 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 Comité Institucional de Coordinación de Control Interno.
Tercera Línea	Control Interno	• 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. • 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 de defensa. • Asesorar a la primera línea de defensa de forma coordinada con el área de Planeación, en la identificación de los riesgos y diseño de controles. • Llevar a cabo el seguimiento a los riesgos consolidados en

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		el mapa de riesgos conforme al Plan Anual de Auditoria y reportar los resultados al CICCI. • Recomendar mejoras a la política de administración de riesgo.

8. NIVEL DE CALIFICACIÓN DE PROBABILIDAD

Tabla 1 *Probabilidad*

Nivel	Probabilidad	Descripción
20%	Muy Baja	La actividad se realiza entre 1 a 4 veces al año.
40%	Baja	La actividad se realiza entre 5 a 24 veces al año.
60%	Media	La actividad se realiza entre 25 a 500 veces al año.
80%	Alta	La actividad se realiza entre 500 a 5000 veces al año.
100%	Muy Alta	La actividad se realiza más de 5000 veces al año.

9. NIVELES DE CALIFICACIÓN DE IMPACTO

La calificación del impacto para los riesgos de gestión y de seguridad de la información se tendrá en cuenta la siguiente escala, de acuerdo con la realidad del Fondo.

Tabla 2 *Impacto*

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
20%	Leve	Pérdida económica hasta 1000 SMLV	Solo de conocimiento de algunos funcionarios.
40%	Menor	Pérdida económica de 1001 hasta 2000 SMLV	De conocimiento general de la entidad a nivel interno, Gerencia General, y Comités
60%	Moderado	Pérdida económica de 2001 hasta 3000 SMLV	Deterioro de imagen con algunos usuarios de relevancia frente a cumplimiento de objetivos
80%	Mayor	Pérdida económica de 3001 hasta 5000 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Territorial.
100%	Catastrófico	Pérdida económica superior a 5000 SMLV	Deterioro de imagen a nivel Nacional con efecto publicitario sostenido a nivel Nacional

La calificación del impacto para los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración establecida por Secretaria de Transparencia de la Presidencia de la Republica. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 3 *Calificación de impacto para los riesgos de Corrupción*

No	Pregunta: Si el riesgo de corrupción se materializa podría….	**RESPUESTA**	
		SI	**NO**
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

No	**Descriptor**	**Descripción**	**Respuestas afirmativas**
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas V5*

10. TRATAMIENTO DE RIESGOS

1.1. Aplicabilidad de tratamiento

- Para todos los tipos de riesgos, son aplicables, en todas sus zonas de riesgo, las opciones de tratamiento de "Reducir", "Compartir" y "Evitar".

- Para los riesgos de corrupción no es aplicable la forma de tratamiento "Aceptar" ni "Transferir", en ninguna de sus zonas de riesgo.

- El tratamiento "Aceptar", solo es aplicable cuando la zona de riesgo inherente o residual es baja, a excepción de los riesgos de corrupción.

1.2. Descripción de tratamiento

A continuación, se expone la descripción de las opciones de tratamiento:

Opción del tratamiento	Descripción
Aceptar	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado). Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.
Reducir	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación o mejora de controles. El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.
Evitar	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.
Compartir	Se reduce la probabilidad o el impacto del riesgo compartiendo una parte de este. Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece

Opción del tratamiento	Descripción
	de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.
Transferir	Se reduce la probabilidad o el impacto del riesgo transfiriendo una parte de este. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

11. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla "acciones de respuesta a riesgos".

Tabla 3. *Acciones de respuesta a riesgos*

Tipo de riesgo	Responsable	Acción
Riesgo de Corrupción y gestión	Líder de proceso	• Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	• Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente.

Tipo de riesgo	Responsable	Acción
		• Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo al procedimiento.

Tabla 4 *Seguimiento al mapa de riesgos y controles*

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento
Riesgos de Gestión, y Seguridad digital	Baja	Se realiza seguimiento SEMESTRAL
	Moderada	Se realiza seguimiento TRIMESTRAL
	Alta	Se realiza seguimiento BIMESTRAL
	Extrema	Se realiza seguimiento MENSUAL
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento MENSUAL	

12. ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento
Riesgos de Gestión, y Seguridad digital	Baja Moderada Alta Extrema	El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de las acciones correspondientes a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.