SUPERINTENDENCIA DE NOTARIADO & REGISTRO
La guarda de la fe pública

POLÍTICA GENERAL PARA LA ADMINISTRACIÓN DE RIESGOS

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código: MP – CNGI – PO – 03 – PL - 01	**Versión: 02**	**Fecha: 31 de Julio de 2024**

EQUIPO DIRECTIVO

Roosvelt Rodríguez Rengifo
Superintendente de Notariado y Registro.
William Pérez Castañeda
Secretaria General.
Alejandro Larreamendy Joerns
Superintendente delegada para el Registro.
Carlos Enrique Melenje Hurtado
Superintendente delegada para el Notariado. (E)
María José Muñoz Guzmán
Superintendente delegado para Protección, Restitución y Formalización de Tierras. (E)
Olman José Olivella Mejía
Director Técnica Registral.
Miguel Alfredo Gómez Caicedo
Director de Vigilancia y Control Notarial.
Carlos Enrique Melenje Hurtado
Director de Administración Notarial.
Martha Páez Canencia
Directora de Talento Humano.
Alejandro Cardona Aguirre
Director de Contratación.
William Pérez Castañeda
Director Administrativa y Financiera. (E)
Sol Milena Guerra
Jefe Oficina de Atención al Ciudadano.
Mauricio Alejandro Rodríguez González
Jefe Oficina Asesora de Planeación.
María José Muñoz Guzmán
Jefe Oficina Asesora Jurídica.

Libertad y Orden

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

1 Introducción

La Superintendencia de Notariado y Registro (SNR) encamina su política de Administración de Riesgos teniendo en cuenta el Modelo Integrado de Planeación y Gestión – MIPG y los instrumentos que el Departamento Administrativo de la Función Pública – DAFP, ha generado para orientar su implementación, así como el Modelo Estándar de Control Interno – MECI, en lo referente a las líneas de defensa.

Esta actualización sigue las orientaciones establecidas por la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 expedida por el DAFP e incorpora las orientaciones estratégicas de la alta dirección, articulando los objetivos estratégicos definidos y el modelo de operación de procesos con la planeación institucional.

La política sigue el principio de que la gestión de los riesgos no es estática, se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de dichos objetivos a través de la toma de decisiones.

La política en general está orientada a los colaboradores de la SNR para realizar la identificación, implementación, control, seguimiento, evaluación y apropiación de los riesgos a los que se encuentra expuesta la entidad, sus controles, acciones de manejo y planes de contingencia, siendo este un instrumento de gestión que permita el uso permanente y el control y monitoreo.

2 Marco Legal

- **Ley 87 de 1993.** Se crea el Sistema Institucional de Control Interno y dota a la administración de un marco para el control de las actividades estatales, directamente por las mismas autoridades.
- **Ley 489 de 1998.** Fortalece el Control Interno, con la creación del Sistema Nacional de Control Interno.
- **Ley 526 de 1999 “Por medio de la cual se crea la Unidad de Información y**

Análisis Financiero

- **Ley 1474 de 2011.** A través de ésta, se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación, sanción de actos de corrupción, la efectividad del control de la gestión pública y ordena que las entidades del orden nacional, departamental y municipal elaboren anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas de mitigación de los riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
- **Ley 1712 de 2014.** Se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, ordena publicar el Plan Anticorrupción y de Atención al Ciudadano.
- **Ley 1753 de 2015.** Integra en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulado con los Sistemas Nacional e Institucional de Control Interno (Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998).
- **Ley 1762 de 2015. "**Por medio de la cual se adoptan instrumentos para prevenir, controlar y sancionar el contrabando, el lavado de activos y la evasión fiscal".
- **Decreto 1083 de 2015.** Determina que las entidades públicas establecerán y aplicarán políticas de administración del riesgo, como parte integral del fortalecimiento de los sistemas de control interno.
- **Decreto 1499 de 2017.** Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades. Actualiza el Modelo Estándar de Control Interno para el Estado Colombiano – MECI a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG (correspondiendo a la 7° Dimensión de MIPG).
- **Decreto 1497 de 2002**. "Por la cual se reglamenta parcialmente la Ley 526 de 1999 y se dictan otras disposiciones"
- **Decreto 830 de 2021** "Por el cual se modifican y adicionan algunos artículos al Decreto número 1081 de 2015, Único Reglamentario del Sector Presidencia de la República, en lo relacionado con el régimen de las Personas Expuestas Políticamente

(PEP)".

3 Objetivo de la Política

Definir los principios básicos para la Administración de Riesgos de la Superintendencia de Notariado y Registro, mediante el establecimiento de la metodología de los diferentes enfoques de riesgo a los que se ve expuesta la Entidad a través de la implementación de controles efectivos en desarrollo de su misión y visión, con el fin de tomar decisiones que contribuyan a la mejora continua.

4 Beneficios de la Política

Considerando que la gestión del riesgo es un proceso efectuado por la Alta Dirección de la Entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la Entidad son los siguientes:

- Apoyar a la toma de decisiones
- Garantizar la operación normal de la Entidad
- Minimizar la probabilidad e impacto de la materialización de los riesgos
- Mejorar la calidad de procesos y procedimientos
- Fortalecer la cultura de control y autocontrol de la Entidad
- Incrementar la capacidad de la Entidad para alcanzar sus objetivos
- Dotar a la Entidad de herramientas y controles para hacer una administración más eficaz y eficiente

5 Alcance de la política

La presente Política *General de Administración de Riesgos*, abarca el manejo de los riesgos asociados a los procesos definidos por la Entidad , que incluyen las siguientes temáticas: de gestión del proceso, de corrupción, de seguridad de la información, de Lavado de activos y Financiación del Terrorismo, fiscal, ambientales, de seguridad y salud en el trabajo, contractuales y de proyectos de inversión, para los cuales se tendrán en

cuenta los lineamientos y metodologías que se definan de acuerdo con el enfoque, por parte de la Segunda Línea de Defensa.

1. Enfoque de los riesgos de gestión del proceso: En todos los procesos identificados en la Entidad.
2. Enfoque de los riesgos de corrupción: En todos los procesos identificados en la Entidad.
3. Enfoque de los riesgos de seguridad de la Información: A todos los activos de información.
4. Enfoque de los riesgos ambientales: A todos los procesos identificados en la Entidad.
5. Enfoque de los riesgos seguridad y salud en el trabajo: A todos los servidores públicos y contratistas de la Entidad.
6. Enfoque de los riesgos contractuales: A todos los procesos contractuales y a los contratos.
7. Enfoque de los riesgos de Proyectos de Inversión: A todos los proyectos de inversión de la Entidad.
8. Enfoque de los riesgos de Lavado de Activos y Financiación del Terrorismo (LA/FT) en todos los procesos en los que se determinen con mayor vulnerabilidad como son el servicio público registral, contratación, talento humano y supervisados
9. Enfoque de los riesgos Fiscales: A todos los procesos identificados en la entidad.
10. Enfoque de Supervisión con enfoque de riesgos: A todos los sujetos vigilados por la Entidad.

Ilustración 1. Enfoque de Riesgos

ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES	Riesgos de Gestión
	Riesgos de corrupción
	Riesgos de Seguridad de la Información
	Riesgos Ambientales
	Riesgos Seguridad y Salud en el Trabajo
	Riesgos Contractuales
	Riesgos de Proyectos de Inversión
	Riesgos de Lavado de Activos y Financiación del Terrorismo.(LA/FT)

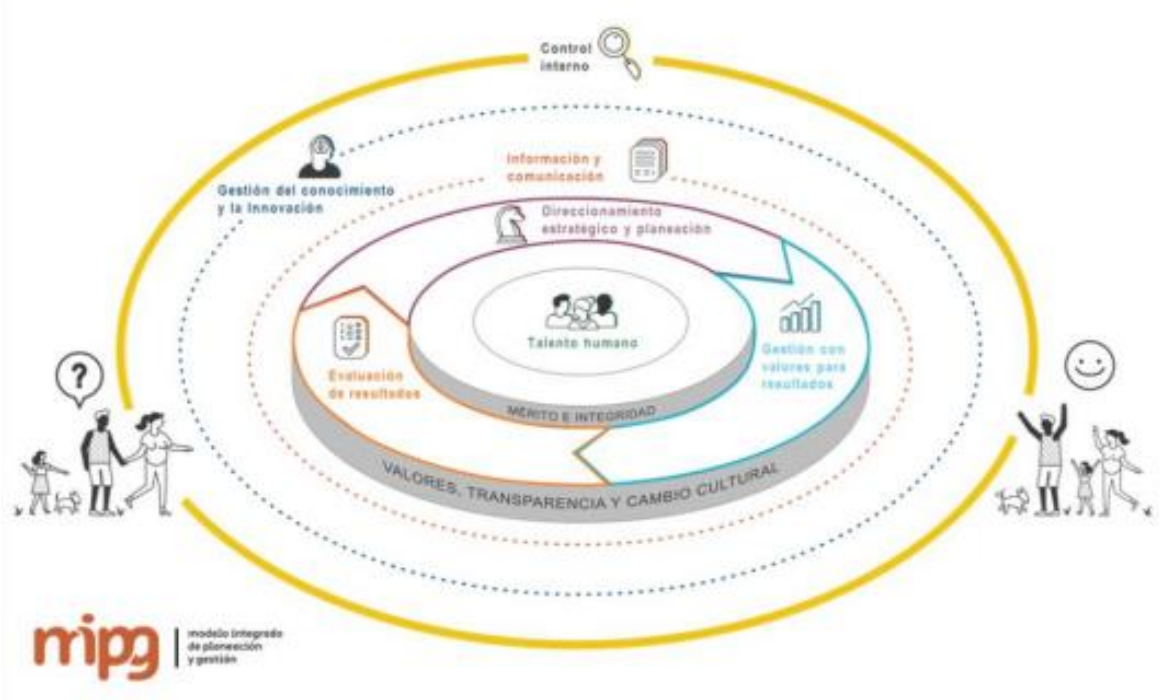
	Riesgos Fiscales

Fuente: Construcción Propia – SNR.

Esta política aplica para todo el personal que labora en la Superintendencia de Notariado y Registro y para los proveedores que participan directamente en la operación. Con esto se mitiga el impacto ante un evento de interrupción que afecte la operación normal de la Entidad.

6 Articulación MIPG con Riesgos

El modelo integrado de planeación y gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, este modelo tiene el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio (Manual operativo MIPG, 2019, p. 6). El MIPG opera a través de 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y, finalmente, control interno) que agrupan las políticas de gestión y desempeño institucional y que, implementadas de manera articulada e interrelacionada, permitirán que el modelo funcione y opere adecuadamente.



Fuente: Departamento Administrativo de la Función Pública, MIPG, 2017.

De acuerdo con el numeral 2.2.1 “política de planeación institucional” de la dimensión “Direccionamiento estratégico y planeación” del MIPG, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

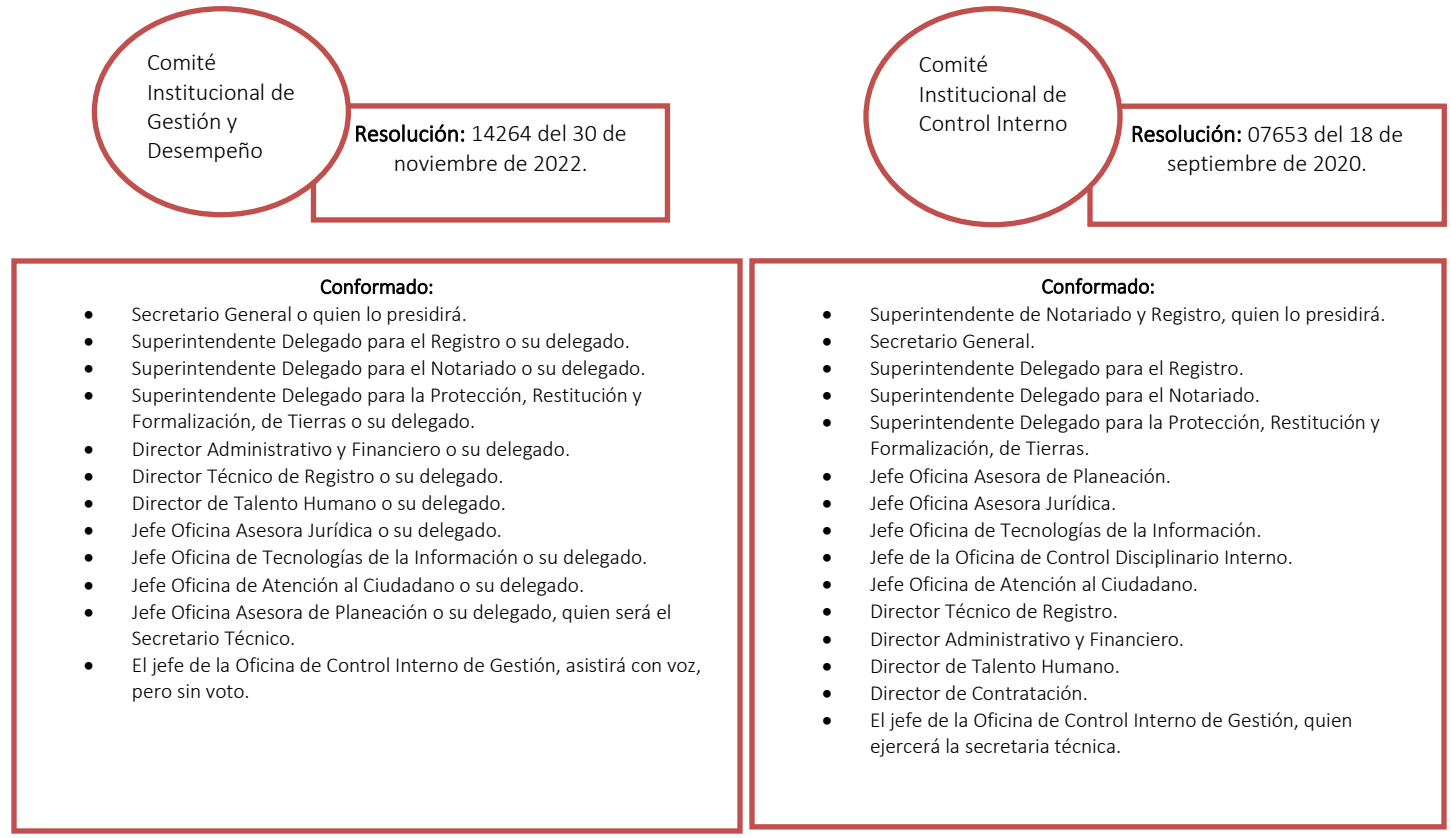
En este sentido, es claro que la identificación y valoración de riesgos se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos.[1]

El Modelo Integrado de Planeación y Gestión (MIPG) define para una operación articulada, la creación del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Control Interno, reglamentado a través

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6

del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en el marco general, para una adecuada gestión del riesgo, los mencionados comités entran a funcionar de la siguiente forma:

Ilustración 2. Operatividad para la Administración del Riesgo.



Fuente: Creación propia

7 Principios de la Política General de Administración de Riesgos

La gestión de riesgos de la Entidad está basada en los siguientes principios:

a) La Entidad es trasparente y no tiene tolerancia a la corrupción. La gestión de riesgos es transparente e inclusiva.

b) La gestión de riesgos contribuye al logro de los objetivos estratégicos y a la mejora del desempeño institucional.

c) La gestión de riesgos hace parte fundamental en la toma de decisiones.

d) La gestión de riesgos es sistemática, estructurada y oportuna.

e) La gestión de riesgos es dinámica, reiterativa y receptiva al cambio. En la medida en que se presenten eventos externos e internos, de su análisis y monitoreo pueden surgir riesgos nuevos y cambios en los ya existentes.

f) La gestión de riesgos se basa en fuentes de información confiable y verificable.

g) La gestión de riesgos toma en consideración los factores humanos y culturales reconociendo las capacidades, percepciones e intenciones de individuos externos e internos, los cuales pueden facilitar o dificultar el logro de los objetivos de la Entidad.

h) La gestión de riesgos facilita la mejora continua de la Entidad.

i) La buena conducta y la ética en el quehacer diario, es un principio esencial en la Entidad. Los servidores públicos y contratistas deben mantener los más altos estándares éticos en sus actuaciones diarias, dentro y fuera de la Entidad.

8 Postulados de la Política General de Administración de Riesgos

El Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno.[2] de la Superintendencia de Notariado y Registro asume el compromiso de impulsar a nivel institucional la cultura y pensamiento basado en riesgos en todos sus procesos, así como la creación y mantenimiento de la cultura de autogestión, autocontrol y autorregulación bajo los siguientes postulados:

a. Se promueve la integración de los diferentes enfoques de riesgo a la cultura institucional, a partir de la divulgación y formación en los temas que componen la

[2] Manual operativo del MIPG. Dimensión. Asignar las responsabilidades para cada componente 7. 7.2.2

administración de riesgos y en las herramientas que se emplean para su gestión.

b. Se consagra como mecanismo fundamental para la prevención y control de los riesgos, la sensibilización permanente de los servidores públicos, contratistas y actores críticos para la Entidad.
c. Se asegura el cumplimiento de las normas internas y externas relacionadas con la administración de riesgos.
d. Se previene y resuelve conflictos de interés en la recolección de información en las diferentes etapas de la Administración de Riesgos de los diferentes enfoques.
e. Considera toda observación de auditoría interna o externa como un riesgo en potencia.

8.1 Postulados sobre los riesgos de corrupción:

La posición de la Superintendencia de Notariado y Registro es de cero tolerancias frente a la corrupción. Por lo anterior, busca permanentemente implementar las mejores prácticas contra estas actividades, en todas las acciones que realiza mediante los siguientes postulados:

a. Considera un riesgo de corrupción materializado cuando se demuestre que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado[3].
b. Se abstiene de participar en cualquier forma o práctica de corrupción, directa o indirectamente.
c. Promueve y establece dentro de toda la Entidad, una cultura institucional anticorrupción.
d. Rechaza que sus servidores públicos, contratistas, proveedores y terceros asociados, obtengan resultados económicos, comerciales o de cualquier otra índole, a cambio de violar la ley o actuar de manera deshonesta.
e. Promueve que los servidores públicos y contratistas cumplan con el Código de Integridad con el fin de prevenir la promoción de cualquier forma de corrupción.
f. Genera un entorno de transparencia, integrando los diferentes sistemas desarrollados para la prevención, detección y respuesta a la corrupción,

[3] Es necesario tener en cuenta la definición de riesgos de corrupción: **"Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado".** - DAFP

manteniendo los canales adecuados para favorecer la comunicación de dichos asuntos al interior de la Entidad y coordinando el conjunto de acciones necesarias para prevenir, detectar y dar respuesta a posibles situaciones de corrupción.

g. Prioriza las actividades de prevención de corrupción, sin disminuir los esfuerzos encaminados a la detección y corrección de situaciones relacionados con los mismos flagelos.
h. Evalúa los indicios de presuntos actos de corrupción, bajo los principios de confidencialidad, integridad, transparencia, objetividad.
i. Tiene en cuenta las quejas y denuncias realizadas por parte de usuarios y funcionarios de la Entidad, para identificar posibles riesgos relacionados con corrupción.
j. Gestiona de forma oportuna todas las denuncias de actos relacionados con corrupción, independientemente de su cuantía o del personal involucrado, garantizando confidencialidad, objetividad, respeto y transparencia. *Ningún funcionario sufrirá consecuencias negativas por prevenir, rechazar o denunciar un acto de esta naturaleza.*
k. Evita vínculos con gerentes públicos, servidores públicos, contratistas, proveedores o terceros asociados que hayan sido condenados por actividades delictivas relacionadas con corrupción.
l. Articula las diferentes normas para la materia, especialmente para el Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (articulo 73) y el Decreto 124 de 2016 (articulo 2.1.4.1.).

8.2 Postulados sobre riesgos LA/FT:

La posición de la Superintendencia de Notariado y Registro es de cero tolerancias frente al lavado de activos y financiación del terrorismo. Por lo anterior, busca permanentemente implementar las mejores prácticas contra estas actividades, en todas las acciones que realiza mediante los siguientes postulados:

a. Considera los riesgos de Lavado de Activos y Financiación del Terrorismo (LA/FT), descritos como la posibilidad de pérdida o daño que podría sufrir la entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el

lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas.

b. Sensibiliza a las partes interesadas, llámese directivos, contratistas y funcionarios en actividades de formación enfocadas a la prevención del riesgo de LA/FT.

c. Evita cualquier tipo de relación con cualquier contraparte que, se encuentre registrado en las listas vinculantes o restrictivas, por medio de las cuales se relacionen a personas tanto naturales como jurídicas en actividades vinculadas con el LA/FT.

d. Controla cualquier tipo de relación con usuarios del servicio público registral para evitar que involucre a la SNR en conductas tipificadas en lavado de activos.

e. Adopta y aplica la inspección, vigilancia y control con enfoque basado en riesgos a sus supervisados, Notarías, Curadurías, Gestores Catastrales y Oficinas de Registro.

f. Garantiza la reserva de la información recaudada y reportada en cumplimiento de lo prescrito en las normas legales vigentes.

g. Los directivos y funcionarios que tengan conocimiento sobre información y documentos de operaciones inusuales o sospechosas tienen el deber de no dar a conocer de tales circunstancias a las personas que realizaron dichas actuaciones.

h. Realiza la debida diligencia frente a personas que se declaren expuestas públicamente (PEP´s), que por razón de su cargo manejan recursos públicos, o tienen poder de disposición sobre éstos o gozan de reconocimiento público las cuales se encuentran relacionadas en el decreto 1674 de 2016.

i. Colabora con la administración de justicia, atendiendo de manera oportuna los requerimientos de las autoridades competentes en materia de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo, de conformidad con lo señalado en el numeral 7º del artículo 95 de la Constitución Política de Colombia que determina como deber de la persona y del ciudadano colaborar para el buen funcionamiento de la administración de la justicia.

j. Dispone los recursos necesarios para garantizar la adecuada gestión de los riesgos que afectan el cumplimiento de los objetivos de la entidad, dando cumplimiento a las regulaciones y requerimientos definidos legalmente.

k. A través, de la Oficina Asesora de Planeación y con el apoyo de quienes

intervengan en los procesos, evalúa el riesgo de LA/FT previo a la incursión de la entidad en nuevos bienes o servicios. Dejará constancia escrita de los resultados obtenidos e impactos.

I. La calificación del impacto para los riesgos de Lavado de Activos y Financiamiento del Terrorismo (LA/FT) se determina mediante el análisis de las respuestas proporcionadas a las 19 preguntas establecidas en la "Guía para la Gestión del Riesgo de Corrupción" de la Presidencia de la República. Estas preguntas se utilizan como una herramienta fundamental para evaluar y comprender la magnitud de los riesgos asociados a la corrupción y a actividades ilícitas de lavado de activos y financiamiento del terrorismo.

8.3 Postulados sobre Riesgos de Seguridad de la Información:

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. 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.
b. Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.
c. La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados.
d. La variable presupuesta es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.
e. La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital.

8.4 Postulados sobre Riesgos Fiscales:

a. La Superintendencia de Notariado y Registro establece la gestión del riesgo fiscal como herramienta para prevenir el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).
b. La gestión del riesgo fiscal en la SNR debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento.
c. La gestión de los riesgos fiscales en la entidad debe permitir una gestión efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite, mitigar la posibilidad de configuración de responsabilidades fiscales.
d. Para la identificación de los riesgos fiscales en la SNR se debe tomar como base el Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas propuesto por el Departamento Administrativo de la Función Pública, el cual contiene aproximadamente 130 fallos con responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República que sirven a nivel de referencia para la identificación y valoración de riesgos fiscales.

9 Niveles de Apetito, Tolerancia y Capacidad Del Riesgo

9.1 Nivel de Apetito de Riesgo de la Entidad

El nivel de apetito de riesgo definido como el nivel de riesgo que la SNR busca asumir para poder lograr sus objetivos, sin necesidad de establecer controles adicionales tendientes a disminuir su probabilidad o su impacto se ha definido de acuerdo con los siguientes criterios.

El análisis para la toma de las decisiones se realiza tomando como base el nivel de riesgo residual a excepción de cuando el análisis se realiza sobre procesos nuevos, frente a lo cual el análisis se realiza con base en el nivel de riesgo inherente.

La entidad solo buscará asumir los riesgos cuyo nivel de riesgo sea evaluado como **BAJO** sin necesidad de establecer medidas adicionales para su mitigación.

Nota: Ningún riesgo de corrupción podrá aceptarse, por lo que ningún riesgo de corrupción se puede evaluar en nivel bajo.

9.2 Nivel de Tolerancia al 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.

Para la SNR la máxima desviación con respecto al nivel de apetito al riesgo definido por la entidad (nivel de riesgo BAJO), corresponde a los riesgos que después de la
aplicación de controles su nivel de riesgo residual sea máximo MODERADO de acuerdo con los criterios de evaluación definidos por la entidad y que se explican en la presente política. Estos riesgos pueden ser admitidos bajo decisión informada por parte de los líderes de los procesos, programas o proyectos siempre que no sea posible establecer medidas adicionales por parte de la entidad o si estas medidas requieren la asignación de presupuestos adicionales importantes o si la adopción de estas nuevas medidas puede dar origen a nuevos riesgos aún mayores que los mitigados por las mismas.

9.3 Capacidad del Riesgo

El máximo nivel de riesgo que puede soportar la SNR antes de que sus objetivos no puedan ser logrados es el Nivel de Riesgo ALTO, todo riesgo que tenga una valoración de ALTO debe ser intervenido a través de un tratamiento del riesgo que permita reducirlo, transferirlo o evitarlo. Un riesgo calificado en esta zona no podrá ser aceptado salvo que se presente una decisión informada por parte del Comité Institucional de Coordinación de Control Interno que como resultado de un análisis del riesgo se determine la imposibilidad para establecer medidas adicionales a las ya aplicadas de acuerdo con la capacidad de gestión de la entidad, o que no sea posible evitar el riesgo dejando de realizar la actividad o actividades que lo generan.

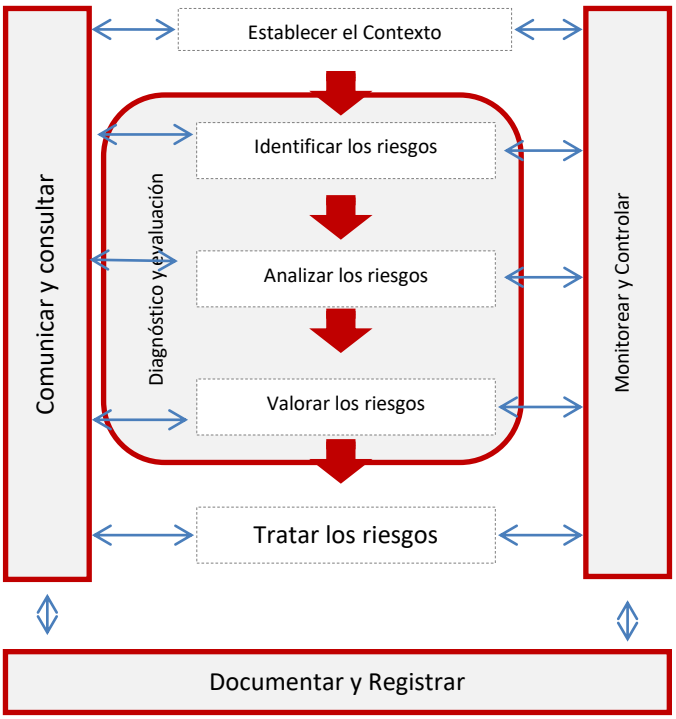
Los riesgos calificados como EXTREMOS no pueden ser admitidos bajo ninguna circunstancia por la entidad debido a que su materialización impediría el logro de

objetivos de la entidad, estos riesgos en todos los casos deben tener medidas de intervención que permitan su mitigación a niveles admisibles de acuerdo con los criterios de evaluación de riesgos definidos en esta política. Si no es posible mitigar o reducir el riesgo, este se debe evitar dejando de realizar las actividades que lo generan.

10 Ciclo de Gestión del Riesgo

La Entidad para el desarrollo y aplicación de la Administración de Riesgos se acoge a las metodologías dadas por el Departamento Administrativo de la Función Pública, las cuales convergen en las siguientes etapas:

Ilustración 3. Ciclo del riesgo



Fuente: Construcción propia

Dichas etapas se encuentran descritas y claras dentro de la “Guía para el diligenciamiento de la matriz de riesgos” código: MP-CNGI-PO-03-PR-01-GI-01 Versión 2, la cual tiene como objetivo proporcionar los lineamientos necesarios a través de una metodología que oriente la identificación, análisis, valoración, tratamiento y seguimiento a los riesgos y a

las oportunidades con el fin de identificar los riesgos de los sistemas y/o procesos en el marco del sistema integrado de gestión.

11 Esquema líneas de defensa para la administración de riesgos

La Entidad se acoge al esquema de asignación de responsabilidades dados por el Modelo Estándar de Control Interno adaptada del modelo de las Líneas de Defensa, el cual es un esquema referencial para describir las responsabilidades y funciones en la administración de los riesgos, mediante líneas de actividad que contribuyan a mejorar la comunicación y coordinación entre los diferentes actores involucrados en el desarrollo de etapas de la gestión del riesgo.

11.1 Línea Estratégica

Responsable: Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno.

Responsabilidades: 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.[4]

La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente:

1. Establecer la política General de Administración de Riesgos, así como las políticas que le aplica de manera particular a cada uno de los sistemas[5] de administración de riesgos que lo componen y asegurarse de su permeabilización en todos los niveles de la Entidad.
2. Revisar los cambios en el “Direccionamiento estratégico” y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
3. Revisar el adecuado desdoblamiento de los objetivos institucionales a los objetivos de

[4] Manual Operativo MIPG V4 – Dimensión de Control Interno.

[5] Entiéndase por sistema, en este contexto, al Sistema de Gestión de Calidad, al Sistema de Seguridad y Salud en el Trabajo, Seguridad de la Información, Riesgos Contractuales, Sistema de Gestión Ambiental y Riesgos de daño Antijurídicos.

procesos, que han servido de base para llevar a cabo la identificación de los riesgos.

4. Hacer seguimiento, a la implementación de cada una de las etapas de la gestión del riesgo y a los resultados de las evaluaciones realizadas por la Oficina de Control Interno.
5. Hacer seguimiento y pronunciarse por lo menos cada cuatrimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo todas las tipologías de riesgos y de acuerdo con las políticas de tolerancia establecidas y aprobadas.
6. Revisar los informes presentados por lo menos cada cuatrimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
7. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
8. Aprobar la metodología para identificar, medir, evaluar y monitorear el riesgo.

11.2 Primera Línea de Defensa

La primera línea de defensa son las áreas originadoras y propietarias de los riesgos y las primeras llamadas a definir y tomar decisiones en cómo gestionarlos. Estas dependencias son responsables de la implementación de acciones preventivas y correctivas para hacer frente a deficiencias del proceso y sus controles.

Responsable: Gerentes Públicos del Nivel Central y las Direcciones Regionales, Registradores de Instrumentos Públicos Principales y Seccionales, Gerentes de Proyectos, Coordinadores de Grupo Interno de Trabajo, Líderes de proceso, Supervisores e Interventores de Contratos y/o Proyectos, responsables de los otros subsistemas de gestión de la Entidad.

Responsabilidades: Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los diferentes enfoques de riesgos con relación a

lo siguiente:

1. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
2. Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos, en el marco de sus procedimientos de supervisión.
3. Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
4. Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño e identificar en caso de que no se estén cumpliendo los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
5. Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos, además se debe actualizar el mapa de riesgos del proceso.
6. Revisar los planes de acción establecidos para cada uno de los riesgos materializados y hacer seguimiento al cumplimiento de las actividades, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento de los objetivos.
7. El monitoreo y revisión periódica de la gestión de riesgos por parte de la primera línea de defensa se hará en las siguientes fechas:

Primer Monitoreo:

Alcance del monitoreo: del 01 de enero al 30 de abril

Fecha de presentación de informe de monitoreo: Dos (2) primeros días hábiles del mes de mayo.

Cargue de evidencias: el cargue de las evidencias de la aplicación de los controles en la OneDrive deberá realizarse permanentemente.

Segundo Monitoreo:

Alcance del monitoreo: del 01 de mayo al 31 de agosto

Fecha de presentación de informe de monitoreo: Dos (2) primeros días hábiles del mes de septiembre.

Cargue de evidencias: el cargue de las evidencias de la aplicación de los controles en la OneDrive deberá realizarse permanentemente.

Tercer Monitoreo:

Alcance del monitoreo: del 01 de septiembre al 31 de diciembre

Fecha de presentación de informe de monitoreo: Dos (2) primeros días hábiles del mes de enero de la siguiente vigencia.

Cargue de evidencias: el cargue de las evidencias de la aplicación de los controles en la OneDrive deberá realizarse permanentemente.

En el tercer monitoreo los procesos de Nivel Central deberán entregar el mapa de riesgos del proceso actualizado para la siguiente vigencia.

11.2.1 Responsabilidades Directores Regionales:

Los Directores regionales como actores definidos en la primera línea de defensa encargados de coordinar la implementación del Sistema de Gestión de Calidad en las Oficinas de Registro de Instrumentos Públicos de su jurisdicción, de conformidad con la normatividad vigente y bajo la orientación del Superintendente de Notariado y Registro y la Oficina Asesora de Planeación[6], tendrán como responsabilidad lo siguiente:

1. Definir estrategias de comunicación y divulgación adecuadas de información relacionada con riesgos a todas la ORIP de su Jurisdicción.
2. Proporcionar asesoramiento y entrenamiento a los servidores públicos y contratistas sobre las herramientas y procedimientos para la gestión del riesgo a las ORIP de su jurisdicción.
3. Realizar seguimiento y supervisión a la adecuada implementación de dichas prácticas por parte de las ORIP de su jurisdicción.

[6] Decreto 2723 Articulo 32 “Funciones de las Direcciones Regionales” Ítem 16: 16. Coordinar la implementación del Sistema de Gestión de Calidad en las Oficinas de Registro de Instrumentos Públicos de su jurisdicción, de conformidad con la normatividad vigente y bajo la orientación del Superintendente de Notariado y Registro y la Oficina Asesora de Planeación.

4. Liderar la formulación del plan de mejoramiento para los casos en los que se identifique la materialización de un riesgo, al igual que la evaluación y seguimiento de las acciones formuladas por las ORIP de su jurisdicción.
5. Generar informe para ser reportado a la Oficina Asesora de Planeación consolidado por Dirección Regional de acuerdo a lo reportado por cada ORIP.
6. Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos, en los siguientes periodos de corte:

Primer Monitoreo:

Alcance del monitoreo: del 01 de enero al 30 de abril.

Fecha de seguimiento: Tres (3) días hábiles después del periodo de corte.

Segundo Monitoreo:

Alcance del monitoreo: del 01 de mayo al 31 de agosto

Fecha de seguimiento: Tres (3) días hábiles después del periodo de corte.

Tercer Monitoreo:

Alcance del monitoreo: del 01 de septiembre al 31 de diciembre

Fecha de seguimiento: Tres (3) días hábiles después del periodo de corte.

11.3 Segunda Línea de Defensa

La segunda línea de defensa soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción y LAFT, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

Responsable: Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo tales como la Oficina Asesora de Planeación para los riesgos de gestión y de corrupción, LAFT, MSER (Modelo de Supervisión Enfocado en

Riesgos), la Oficina de Tecnologías de la Información para los riesgos de Seguridad de la Información, la Dirección Administrativa y Financiera para los riesgos ambientales, la Dirección de Talento Humano para los riesgos de Seguridad y Salud en el Trabajo, la Dirección de Contratos para los riesgos contractuales, los gerentes de proyectos de inversión para los riesgos de proyectos de inversión, la Dirección Técnica de Registro para las ORIP y Directores Regionales.

Responsabilidades: Deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, con relación a lo siguiente:

1. 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 solicitar y apoyar en la actualización de las matrices de riesgos.
2. Orientar a las instancias de dirección en el marco más adecuado para la gestión de riesgos (políticas, alcance, principios y estructura organizacional).
3. Formular la metodología que será empleada por la primera línea de defensa para gestionar adecuadamente los riesgos a los que se ven expuestos.
4. Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
5. Acompañar a la primera línea de defensa en el diseño de controles para la gestión de riesgos y problemas, aportando su visión independiente.
6. Proporcionar asesoramiento y entrenamiento sobre las herramientas y procedimientos empleados para la gestión del riesgo a los procesos institucionales del nivel central y a las cinco (5) direcciones regionales.
7. 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 determinar las recomendaciones y seguimiento para el fortalecimiento de estos.
8. Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la Entidad.
9. Aprobar los mapas de riesgos de los diferentes enfoques y con ellos, elaborar el mapa

de riesgos institucional y el mapa de riesgos de corrupción.

10. Revisar los planes de acción 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 vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.
11. Definir estrategias de comunicación y divulgación adecuadas, en la cual se presente información relacionada con riesgos a toda la Entidad a través de la página web institucional.
12. Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos, en los siguientes periodos de corte:

Primer seguimiento:

Alcance del monitoreo: del 01 de enero al 30 de abril.

Fecha de seguimiento: Cinco (5) días hábiles después del periodo de corte.

Segundo seguimiento:

Alcance del monitoreo: del 01 de mayo al 31 de agosto

Fecha de seguimiento: Cinco (5) días hábiles después del periodo de corte.

Tercer seguimiento:

Alcance del monitoreo: del 01 de septiembre al 31 de diciembre

Fecha de seguimiento: Cinco (5) días hábiles después del periodo de corte.

11.4 Tercera Línea de Defensa

Responsable: Oficina de Control Interno de Gestión.

Responsabilidades: La Oficina de Control Interno tiene como principal función, verificar la adecuada gestión de riesgos dentro de la Entidad de manera independiente a la primera y segunda línea de defensa, así como:

1. 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.

2. Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
3. Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
4. Revisar el adecuado diseño y ejecución 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.
5. Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no sea coherente con los resultados de las auditorías realizadas.
6. Revisar que como resultado de las auditorías efectuadas se encuentren actualizados y documentados cada uno de los procedimientos, así como los planes de mejora se lleven a cabo de manera oportuna estableciendo la causa raíz del problema evitando en lo posible la repetición de hallazgos y la materialización de riesgos.

11.5 Servidores públicos y/o contratistas

1. Conocer los riesgos del proceso del cual hacen parte dentro de la entidad.
2. Generar las alertas tempranas para evitar la materialización de los riesgos.
3. Seguir las políticas, procedimientos y controles establecidos para prevenir la materialización del riesgo de corrupción.
4. Los servidores públicos y terceros que de buena fe reporten hechos sospechosos serán protegidos; La Superintendencia de Notariado y Registro no tomará represalias contra los denunciantes y mantendrá la confidencialidad de las denuncias ajustándose en un todo a la Ley.
5. Los gerentes públicos, registradores de Instrumentos Públicos Principales y seccionales servidores público, contratistas y terceros asociados de la Superintendencia de Notariado y Registro tienen la responsabilidad de aplicar los

principios de autocontrol, autogestión y autorregulación, como parte integral en el desarrollo de sus actividades, así como la responsabilidad de reportar toda sospecha de deshonestidad, todo evento de corrupción del que tenga conocimiento así como cualquier debilidad de control.

12 Divulgación de la Información

1. La Superintendencia de Notariado y Registro debe divulgar a través de su página web la información relevante y necesaria, con el fin que los ciudadanos puedan conocer las estrategias de administración general de riesgos.
2. El vocero único de la Superintendencia de Notariado y Registro es el Superintendente, ningún servidor público, colaborador o contratista se encuentra autorizado para divulgar información de la Entidad, sin su previa autorización.
3. La divulgación interna y externa en materia de riesgos debe cumplir con los lineamientos establecidos por la Entidad en cuanto a mantener la seguridad, calidad y confidencialidad de la información.
4. La revelación contable se debe realizar en los términos de Ley y bajo los correspondientes principios contables que regulan la materia. Al cierre de cada ejercicio contable, la administración debe incluir en el informe de gestión, los aspectos destacados de la administración General de los riesgos.
5. Para efectos de divulgación de la información interna, se deben utilizar como medios de comunicación el correo institucional y las herramientas tecnológicas que soporten la administración del Sistema Integrado de Gestión - SIG, en lo que respecta a la publicación de los manuales, procesos y demás documentos relacionados con el sistema General de Administración de Riesgos y Oportunidades, sus partes y anexos.

12.1 Capacitación sobre las metodologías de Riesgos.

1. La capacitación sobre la Administración de Riesgos deberá estar contenida en el programa de inducción y reinducción institucional, la cual es liderada por la Dirección de Talento Humano.
2. Todos los servidores públicos y colaboradores de la Entidad durante el proceso de inducción y reinducción deben recibir capacitación sobre la administración general de

riesgos haciéndolos responsables de su adecuado funcionamiento.

3. La formación en materia de administración general de riesgos es obligatoria para todos los servidores públicos de la Entidad.
4. Los servidores públicos y colaboradores de la Entidad que tienen roles concretos en la gestión de riesgos deben recibir capacitación específica y de acuerdo con las necesidades propias de sus funciones y responsabilidades.
5. Los programas de capacitación en relación con el sistema de administración de riesgos se deben realizar mínimo una vez al año.

13 Análisis y Evaluación del Riesgo

Para el análisis de riesgos se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias e impacto.

13.1 Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.7

Tabla 1. 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%

[7] Guía para la administración del Riesgo y el diseño de controles en entidades públicas, Versión 6. (Paso 3. Valoración del Riesgo)

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

13.2 Determinar Impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado. Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Tabla 2. 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.

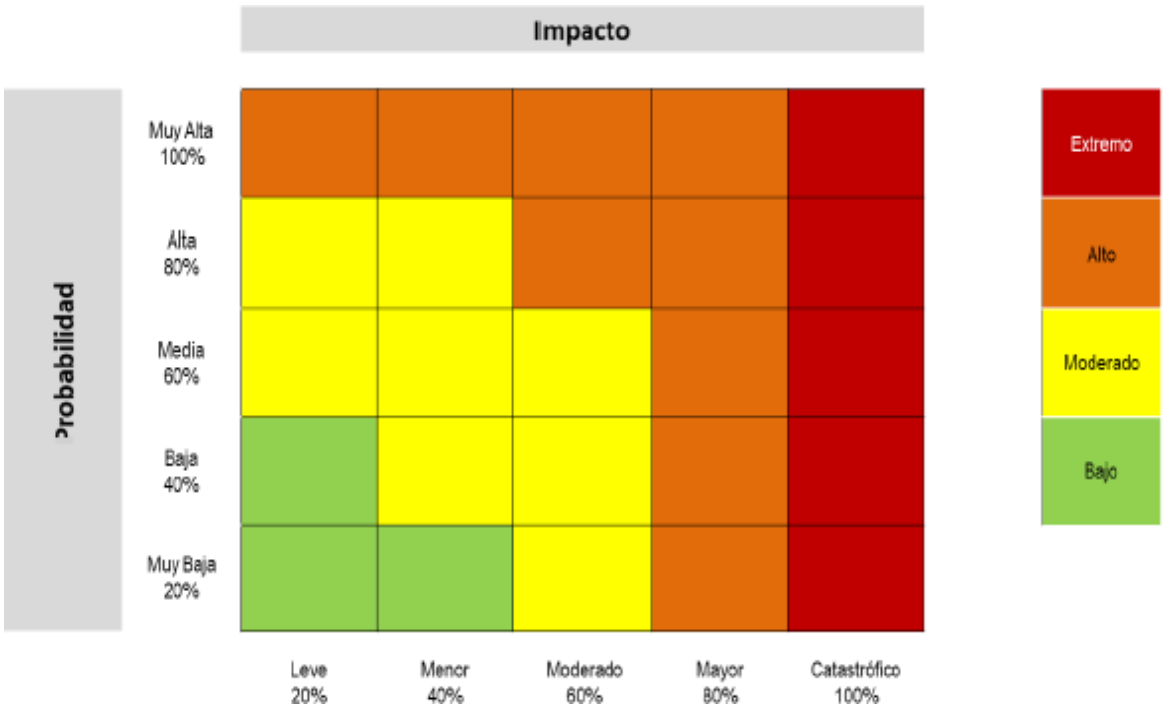
IMPORTANTE: Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite

para el impacto, ya que no se trata de un análisis subjetivo. Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.[8]

13.3 Mapa Zonas de Calor de la Entidad

A continuación, se presentan los mapas de zonas de calor para los riesgos de la SNR los cuales muestran las zonas de calor en la cuales se puede ubicar un riesgo una vez calificado en cuanto a probabilidad e impacto.

Mapa1. Zonas de Calor para Riesgos de Institucionales

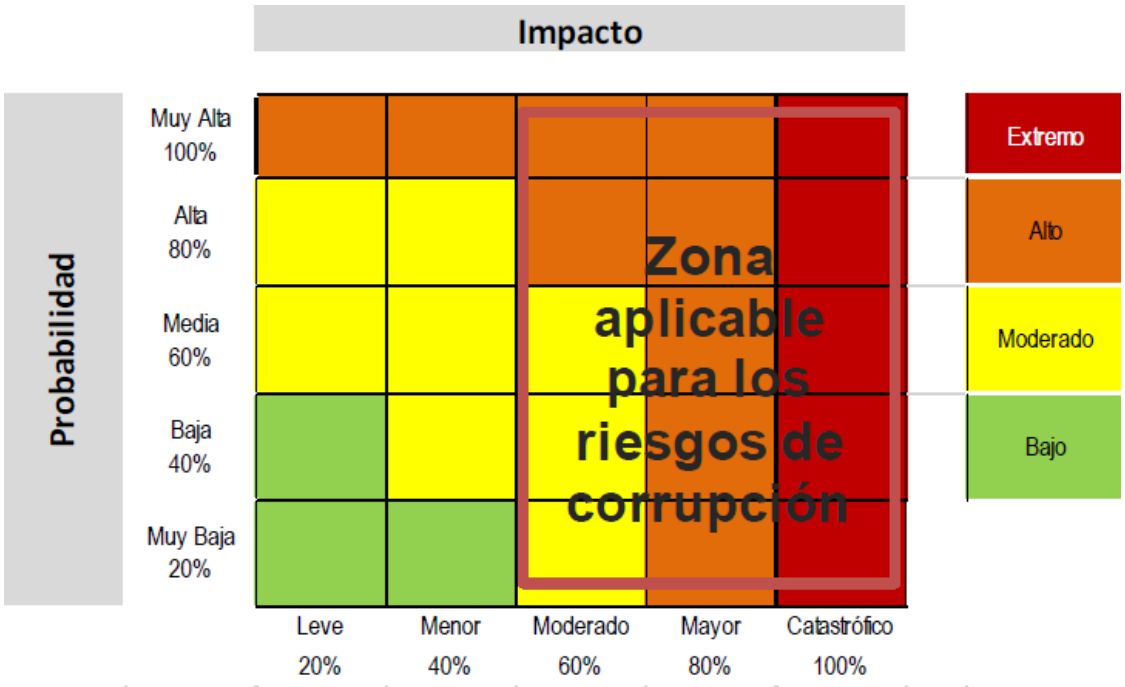


Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

[8] Guía para la administración del Riesgo y el diseño de controles en entidades públicas, Versión 6. (Paso 3. Valoración del Riesgo).

Para los riesgos de corrupción los impactos en ningún caso pueden ser calificados como leves o menores, por lo que para el mapa de calor de los riesgos de corrupción no aplican las dos primeras columnas del mismo, así como se presenta en la siguiente gráfica.

Mapa 2. Zonas de Calor para Riesgos de Corrupción



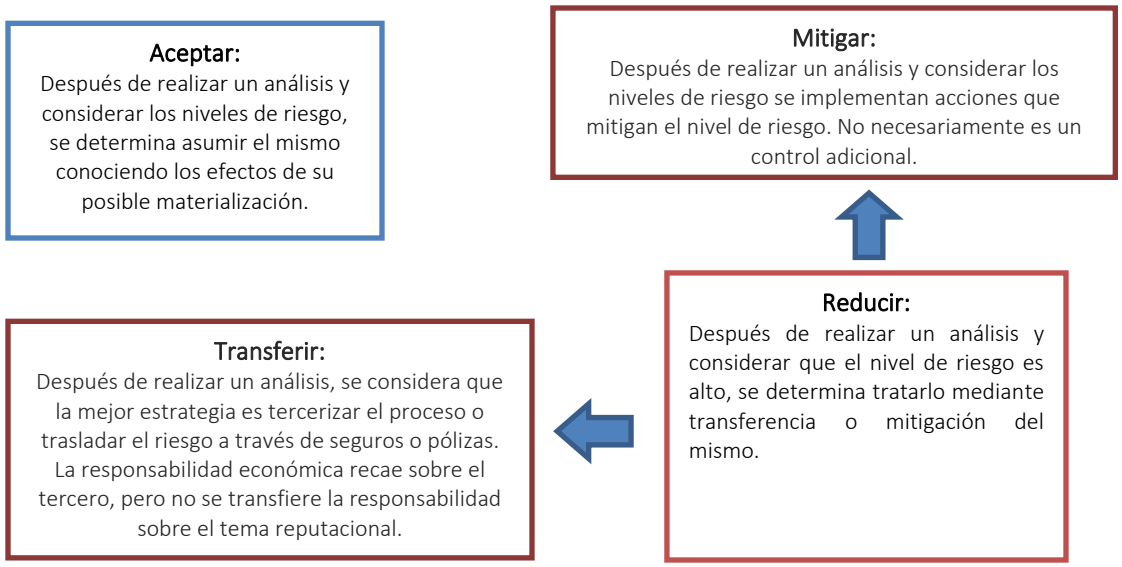
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

14 Medidas para Combatir los Riesgos

Corresponden a las decisiones que se toman frente a un determinado nivel de riesgo, estas pueden ser aceptar, reducir o evitar los riesgos. 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 siguiente ilustración se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Ilustración 4. Estrategias para combatir el riesgo



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

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad del Negocio[9] y se consideraría un control correctivo.

Con base en los resultados de la evaluación del riesgo, este se ubicará en la zona *extrema, alta, moderada o baja*; la mencionada categoría ayuda a determinar la acción requerida asociada a la eliminación de las causas y al fortalecimiento de los controles existentes. Es importante citar que cada tipología de riesgo cuenta con sus propios criterios de valoración e impacto, descritos en la Guía para la identificación de riesgos, oportunidades, evaluación del diseño y efectividad de controles.

Se admite la existencia del riesgo si este se encuentra en una zona de riesgo residual "Baja"; el responsable de administración puede ***aceptar*** las posibles consecuencias, si estas no afectan de manera importante o grave el logro de los objetivos del proceso, sin embargo, debe garantizar la aplicación de los controles existentes y mantener el riesgo monitoreado.

Aquellos riesgos que se ubiquen en otra zona deberán implementar acciones encaminadas a ***reducir*** el nivel de riesgo, bien sea mejorando controles existentes o implementando nuevos controles, o ***transfiriendo*** el riesgo.

Zona de Riesgo Inherente		**Zona de Riesgo Residual**	
Extremo	**Tratamiento:** Desarrollo de las actividades de control	Extremo	**Tratamiento para reducir el riesgo** Plan de mejoramiento para mejorar los controles existentes o crear nuevos controles
Alta		Alta	
Moderado		Moderado	
Bajo	**Tratamiento:** Desarrollo de las actividades de control	Bajo	**Tratamiento** desarrollo de actividades de control

[9] 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.

Nota:

1. Para los riesgos de corrupción y de LA/FT la tolerancia **es inaceptable.**
2. La definición e implementación de acciones eficaces orientadas a reducir o transferir los riesgos identificados deberán contemplar la viabilidad técnica, jurídica y financiera para su implementación.
3. Para riesgos que no tienen una opción de tratamiento inmediata, se debe generar un análisis por parte del Líder del Proceso para definir el plan de mitigación más apropiado; estos riesgos deben permanecer en constante monitoreo.
4. Cuando un riesgo se materializa el proceso debe elaborar un plan de mejoramiento que involucre - entre otros aspectos- el análisis, evaluación, tratamiento, monitoreo y revisión del evento y revisión de controles.
5. Para definir acciones en caso de materialización de riesgos de gestión, en el evento de materializarse un riesgo de gestión, es necesario realizar los ajustes necesarios con acciones, tales como:
    a. Revisar y actualizar el mapa de riesgos, en particular, las causas generadoras del evento y la aplicación de los controles.
    b. Suscribir plan de mejoramiento y realizar el análisis de causas.
    c. Elaborar plan de contingencia respectivo.
    d. Llevar a cabo un monitoreo cuatrimestral permanente por una vigencia.

15 Controles para Mitigar los Riesgos

Los controles hacen referencia a las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Los controles se estandarizan y despliegan a través de la información documentada de la entidad sin embargo un documento como una política, un manual o un procedimiento no es por sí solo un control.

Los controles por sí solos permiten prevenir la materialización del riesgo o mitigar los posibles impactos, por lo que actividades como sensibilizaciones, capacitaciones o acompañamientos no se consideran actividades de control.

Los controles están asociados a actividades como validaciones, verificaciones, seguimientos, chequeos, activación de planes de contingencia, activación planes de continuidad, ejecución de pólizas entre otros.

La identificación y aplicación de controles para la prevención y mitigación de los riesgos es responsabilidad de los líderes de los procesos en conjunto con sus equipos (primera línea de defensa, este ejercicio de identificación y diseño de controles debe estar acompañado desde la Oficina Asesora de Planeación (segunda línea de defensa)

Nota. Es responsabilidad de la tercera línea de defensa evaluar los controles en su efectividad.

15.1 Tipos de Controles

Los controles se pueden clasificar mediante dos grandes criterios: de acuerdo con su propósito y de acuerdo con su forma de ejecución

De acuerdo con su propósito, los controles se clasifican en tres tipos:

Los Controles Preventivos: Son los controles que están diseñados para evitar la materialización de un riesgo que pueda afectar el cumplimiento de los objetivos.
Los controles preventivos deben atacar las causas del riesgo, por lo que cada causa debe tener asociado al menos un control.

Los controles preventivos permiten disminuir el nivel de probabilidad del riesgo.

Ejemplo: La revisión que hace el supervisor del contrato para evitar que se presente un posible incumplimiento de las obligaciones contractuales por parte del contratista.

Los Controles Detectivos: Son los controles que están diseñados para detectar una posible materialización de un riesgo.

Al permitir la detección oportuna antes de la materialización de un riesgo, estos controles pueden evitar la materialización del mismo, pero generan reprocesos. Estos controles disminuyen la probabilidad del riesgo.

Ejemplo: Las conciliaciones que se realizan para detectar inconsistencias en la información contable o financiera antes de emitir informes financieros.

Los Controles Correctivos: Estos controles corresponden a acciones que se ejecutan después de que un riesgo se materializa.

Estos controles disminuyen el nivel de impacto de los riesgos.

Ejemplo: Las pólizas de cumplimiento que se aplican en los casos en los que se materializa el incumplimiento de un contrato y que busca mitigar el impacto económico del incumplimiento.

De acuerdo con forma de ejecución:

Los Controles Manuales: Estas actividades de control son ejecutadas directamente por los servidores de la entidad.

Ejemplo: La supervisión de la ejecución de un contrato por parte del respectivo supervisor del contrato.

Los Controles Automáticos: El control se aplica mediante un aplicativo o un sistema de información de manera automática.

Ejemplo: Conciliaciones contables automáticas realizadas por el aplicativo contable y que arroja errores que deben ser corregidos.

15.2 Planes de Contingencia

Un plan de contingencia es un conjunto de acciones y recursos p*ara responder a las fallas e interrupciones* específicas de un proceso, se establece para ser ejecutado en caso de que el riesgo se materialice o en casos de *sobrepasar el nivel de tolerancia* o exceder los límites de exposición al riesgo fijado; Deben elaborar plan de contingencia todos aquellos procesos que:

1. Estén expuestos a eventos de corrupción cuyo riesgo se encuentre en zona extrema.
2. Aquellos procesos cuya materialización del riesgo afecte de manera directa el servicio al ciudadano e impida la continuidad del servicio.
3. Aquellos procesos cuya materialización del riesgo exponga la integridad física de una persona.

15.2.1 Protocolo de contingencia para la materialización de un riesgo de

corrupción

Con ocasión de los eventos relacionados en los Postulados de la política general de administración de riesgos, (literal a. “se deberán activar los protocolos de contingencia de manera inmediata”) y los hallazgos derivados de denuncias[10] o la presunta comisión de determinada falta delito o contravención deberán estar sujetas a la confirmación del ilícito por parte de la autoridad competente, para qué, se dé lugar a la confirmación del hallazgo y, por ende, a la activación de protocolos de contingencia**.**

En caso de haberse identificado la materialización de un acto de corrupción, la primera línea de defensa correspondiente, realizará el análisis de causa raíz del proceso afectado que dio origen a la materialización del riesgo, valorando el diseño de los controles y su aplicación; y se activara de manera inmediata la Línea de Defensa Estratégica a través del Comité Institucional de Coordinación de Control Interno los cuales sesionarán para analizar la situación y seguir las siguientes actividades:

1. Realizar una evaluación del análisis de causas raíz presentado por la primera línea de defensa del proceso afectado y determinar que el hecho obedece a los eventos de los Postulados de la política general de administración de riesgos.
2. Reubicar al servidor público en un proceso diferente o donde la exposición al riesgo sea baja mientras se adelanta la investigación respectiva.
3. Dar traslado a los entes externos de control o investigación (Procuraduría General de la Nación, Contraloría General de la República, Fiscalía General de la Nación) y a la Oficina de Control Disciplinario Interno, para que adelanten las acciones pertinentes a que haya lugar.
4. Priorizar que, en el marco de las investigaciones disciplinarias de corrupción, las dependencias de la SNR brinden la asistencia oportuna e inmediata, a la aplicación de protocolos de contingencia y práctica de pruebas por parte de la OCDI de la SNR y demás autoridades competentes, con el fin de minimizar el impacto del riesgo cumplido.
5. En caso de que el riesgo de corrupción se presente en una ORIP se activará el

[10] Denuncia sobre conductas irregulares: A través del aplicativo de institucional de tratamiento a las P.Q.R.S.D., se recibirán las denuncias tanto internas como externas, sobre presuntas conductas irregulares.

procedimiento de *visitas especiales* desarrollada por la Superintendencia Delegada para el Registro con enfoque a riesgos.

6. Minimizar el impacto a través de los medios de divulgación y comunicación institucional, sin exponer la investigación y sin dañar el buen nombre del investigado.
7. Llevar a cabo un monitoreo mensual permanente por una vigencia, por parte del responsable del proceso donde se materializó el riesgo, verificando la ejecución de los controles.

16 Disposiciones para la Transición de la Implementación de la Nueva Versión de la Nueva Política General de Administración del Riesgo

Una vez se apruebe, publique y divulgue la nueva versión de la Política General de Administración del Riesgo iniciará el periodo de transición para su implementación de acuerdo con las siguientes disposiciones:

- La implementación de los lineamientos definidos en la presente política se realizará en el marco del ejercicio del rediseño de los procesos, toda vez la gestión del riesgo debe atender el modelo de operación por procesos de la entidad de acuerdo con lo establecido en la guía para la administración del riesgo en entidades públicas versión 6 del DAFP.
- La nueva versión de los mapas de riesgos institucionales resultantes de la aplicación de la presente política entrará en vigencia una vez se terminé el proceso de actualización de los mapas de riesgos con todos y cada uno de los procesos y demás información documentada de la entidad y estos sean formalizados y publicados.
- Los ejercicios de monitoreo, seguimiento, auditorías y aseguramiento de los riesgos de la entidad se realizarán con base en la política que cobija los mapas de riesgos vigentes hasta tanto no entren las nuevas versiones de mapas de riesgos institucionales en vigencia de acuerdo con la disposición anterior. Esto para no generar desfases entre la versión de la política y los mapas de riesgos vigentes.

17 Glosario de términos

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Apetito 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 de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **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.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el 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.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Corrupción:** Cualquier acción u omisión cometida por un servidor, colaborador o tercero de la entidad, usando el poder con el fin de desviar la gestión hacia un beneficio particular. De acuerdo con las definiciones establecidas, la corrupción es una clasificación del fraude, que implica una calificación del sujeto que realiza el acto, teniendo en cuenta que son personas con poder o incidencia en la toma de decisiones y la administración de los recursos de la Entidad.
- **Evento:** Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.
- **Fraude:** Cualquier acción u omisión intencional realizada con el fin de obtener un provecho económico ilícito, en detrimento de los intereses de la entidad o de un tercero.
- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización

con respecto al riesgo.

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **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.
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Plan de contingencia:** Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.
- **Plan de continuidad del negocio:** Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **Riesgo de 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 inherente:** Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. El riesgo inherente puede reducirse de acuerdo con la gestión

operativa de la entidad, lo cual se hace a través de la adopción de políticas, procesos, procedimientos, y definición de perfiles de los funcionarios previos a su contratación entre otros.

- **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Servidor Público:** Son servidores públicos los miembros de las corporaciones públicas, los empleados y trabajadores del Estado y de sus entidades descentralizadas territorialmente y por servicios. Los servidores públicos están al servicio del Estado y de la comunidad; ejercerán sus funciones en la forma prevista por la Constitución, la ley y el reglamento.
- **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.
- **Tratamiento al riesgo:** Es la acción que la entidad toma para prevenir o mitigar los impactos de eventos que afectaría el logro de objetivos, mediante una apropiada definición e implementación de controles, de manera que los riesgos se sitúen en un nivel tolerable por la institución.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
- **Lavado de activos y financiación del terrorismo**: El lavado de activos y la financiación del terrorismo (LA/ FT) son delitos que consisten en el movimiento de recursos de origen y/o destino ilícito. Ambas actividades, asociadas a distintas manifestaciones criminales, se basan en eludir los controles del Estado, utilizando todos los canales económicos a su disposición, tanto financieros como del sector real.
- **Programa de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo**: es una herramienta diseñada para identificar, evaluar, mitigar y monitorear los riesgos de lavado de activos y financiamiento del terrorismo en entidades financieras y otras organizaciones sujetas a regulación. La integración del SARLAFT en la política general de administración de riesgos permitirá a la entidad adoptar un enfoque efectivo en la gestión de los riesgos asociados con el lavado de activos y financiamiento del terrorismo. Al utilizar esta estrategia integral, la entidad estará mejor preparada para enfrentar y prevenir posibles amenazas, protegiendo así su integridad y contribuyendo a la lucha contra actividades ilícitas financieras y

terroristas.

18 Bibliografía

- ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

- Departamento Administrativo de la Función Pública. (2022). GUIA PARA LA ADMINISTRACIÓN DL RIESGO Y EL DISEÑO DE CONTROLES EFICACES EN ENTIDADES PUBLICAS VERSIÓN 6. Bogotá D.C.

19 Anexos: No aplica

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**
DE - SOGI – PR – 07 - GI -01	1	20/08/2019	Se actualiza de conformidad con la nueva metodología de riesgos, dada por el Departamento Administrativo de la Función Pública.
DE - SOGI – PR – 07 - GI -01	2	24/04/2020	Se actualiza de conformidad con la nueva metodología de riesgos, dada por el Departamento Administrativo de la Función Pública.
MP - CNGI – PO – 03 - PL - 01	1	17/03/2022	Se actualiza de conformidad con la nueva metodología de riesgos, dada por el Departamento Administrativo de la Función Pública y de acuerdo con la nueva estructura del Mapa de Procesos de la Entidad.
MP - CNGI – PO – 03 - PL - 01	2	31/07/2024	Se actualiza de conformidad con lo nuevos lineamientos que en materia de gestión de riesgos debe implementar la entidad, atendiendo las directrices del Departamento Administrativo de la Función Pública y en el marco de su modelo de operación por procesos.

ELABORACIÓN Y APROBACIÓN						
ELABORÓ		**REVISIÓN METODOLÓGICA**		**APROBÓ**	**Vo. Bo Oficina Asesora de Planeación**	
Rodrigo Barrero Muñoz Andrés Chíquiza Cuervo	Contratista Oficina Asesora de Planeación. Contratista Oficina Asesora de Planeación.	Rodrigo Barrero Muñoz Andrés Chíquiza Cuervo	Contratista Oficina Asesora de Planeación. Contratista Oficina Asesora de Planeación.	Mónica Yaneth Galvis García Coordinadora Grupo de Arquitectura Organizacional y Mejoramiento Continuo de la Oficina Asesora de Planeación	Mónica Yaneth Galvis García	Coordinadora Grupo de Arquitectura Organizacional y Mejoramiento Continuo de la Oficina Asesora de Planeación
Fecha: 13 de Junio de 2024		Fecha: 17 de Julio de 2024		Fecha: 31 de Julio de 2024	Fecha: 31 de Julio de 2024	