

Gestión del Riesgo

¿QUÉ ES?

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

¿QUIÉN LA ESTABLECE?

La Alta Dirección de la entidad
 Con el liderazgo del representante legal
 Con la participación del Comité Institucional de Coordinación de Control Interno

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

¿QUÉ SE DEBE TENER EN CUENTA?

Objetivos estratégicos de la entidad
 Niveles de responsabilidad frente al manejo de riesgos
 Mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad

¿QUÉ DEBE CONTENER?

Objetivo:	Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
Alcance:	La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información (ver caja de herramientas)
Niveles de aceptación al riesgo:	Decisión informada de tomar un riesgo particular (NTC GTC137, Numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.
Niveles para calificar el impacto:	Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario coniderar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).
Tratamiento de riesgos:	Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.).
Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual.	

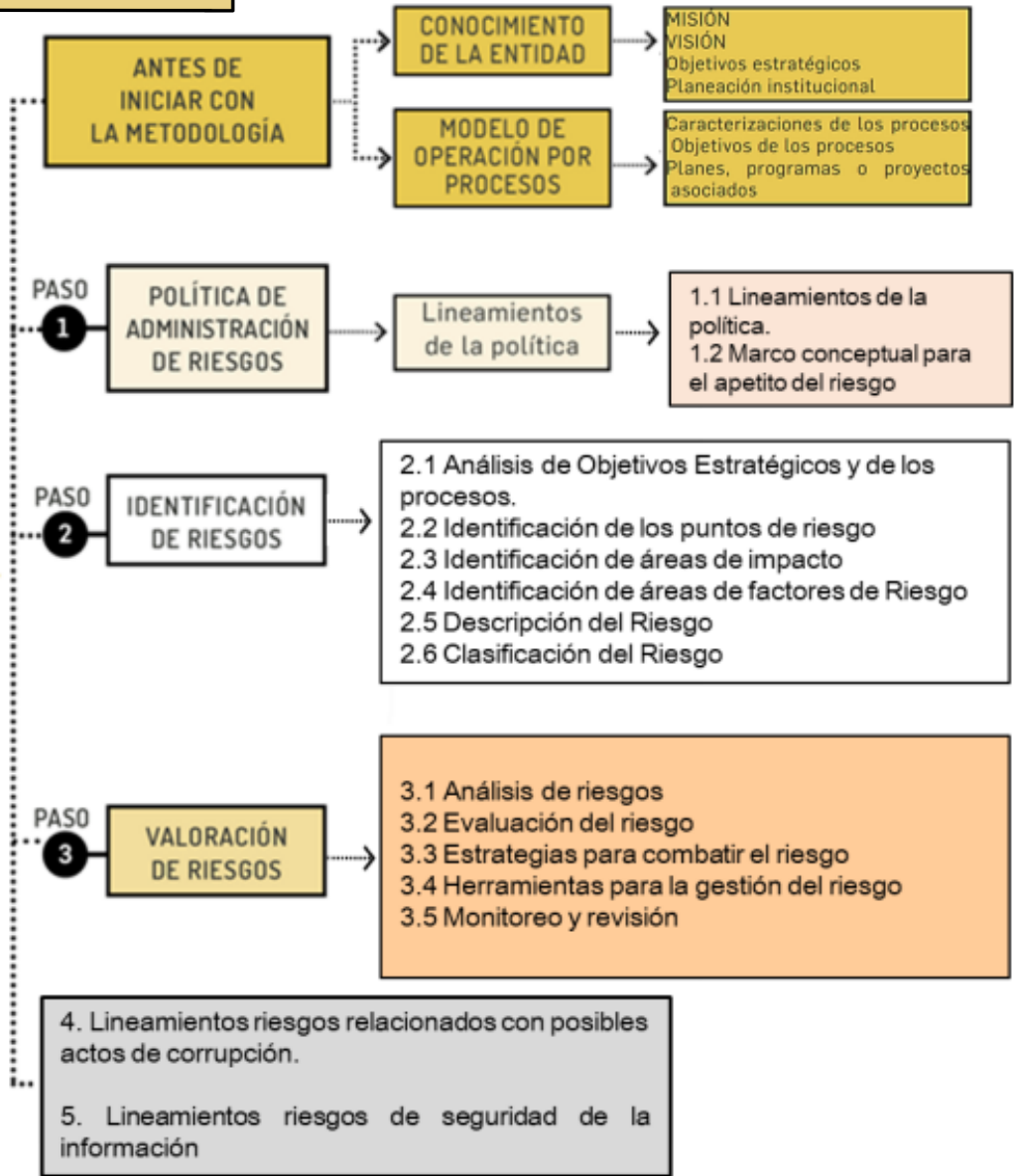
IMPORTANTE

El MIPG establece que esta es una tarea propia del equipo directivo y se debe hacer desde el ejercicio de "Direccionamiento estratégico y de planeación". En este punto, se deben emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

Adicional a los riesgos operativos, es importante identificar los riesgos de corrupción, los riesgos de contratación, los riesgos para la defensa jurídica, los riesgos de seguridad digital, entre otros.

La aceptación del riesgo puede ocurrir sin tratamiento del riesgo. Los riesgos aceptados están sujetos a monitoreo. Tenga en cuenta que los riesgos de corrupción son inaceptables.

METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS



ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

Determina los siguientes aspectos:

- * La metodología a utilizar.
- * En caso de que la entidad haya dispuesto un software o herramienta para su desarrollo, deberá explicarse su manejo.
- * Incluir los aspectos relevantes sobre los factores de riesgo estratégicos para la entidad, a partir de los cuales todos los procesos podrán iniciar con los análisis para el establecimiento del contexto.
- * Incluir todos aquellos lineamientos que en cada paso de la metodología sean necesarios para que todos los procesos puedan iniciar con los análisis correspondientes.
- * Incluir la periodicidad para el monitoreo y revisión de los riesgos, así como el seguimiento de los riesgos de corrupción,
- * Incluir los niveles de riesgo aceptados para la entidad y su forma de manejo.
- * Incluir la tabla de impactos institucional (ver tabla ilustrativa 3. Niveles para calificar el impacto o consecuencias, p. 31).
- * Otros aspectos que la entidad considere necesarios deberán ser incluidos, con el fin de generar orientaciones claras y precisas para todos los funcionarios, de modo tal que la gestión del riesgo sea efectiva y esté articulada con la estrategia de la entidad.

1



OBJETIVO

Establece los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrenta la entidad.

2



ALCANCE

Establece el ámbito de aplicación de los lineamientos, el cual debe abarcar todos los procesos de la entidad. Se sugiere incluir a todas las seccionales o sedes que la entidad pueda tener en diferentes ubicaciones geográficas, con el fin de garantizar un adecuado conocimiento y control de los riesgos en todos los niveles organizacionales.

3



TÉRMINOS Y DEFINICIONES

Aquellos relacionados con la administración del riesgo y con los temas que el manual o guía desarrollen y sean relevantes para que todos los funcionarios entiendan su contenido y aplicación.

