



MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS

AP-MAN-003

HOJA DE APROBACIÓN

Datos	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	José Gilberto Molina Pacavita Luz Adriana Prieto Bárceñas	Carlos Andrés Gutiérrez Basto	Angela María Moncada Arias
Cargo:	Profesionales Especializados de la Dirección Seguimiento y Mejoramiento de Procesos	Coordinador Gestión de Procesos y Riesgos	Directora Seguimiento y Mejoramiento de Procesos
Fecha:	27/11/2025	28/11/2025	30/11/2025

HOJA DE CONTROL DE CAMBIOS

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
1.0	Creación	05/12/2018	Creación del Manual	Todos	Carlos Andrés Gutiérrez Basto
2.0	Cambio de fondo	26/11/2024	<ul style="list-style-type: none">Se cambia la codificación del documento a AP-MAN-003 para adecuarlo a los lineamientos de codificación de documentos del SIG.Se incluye la identificación, valoración y tratamiento de riesgos fiscales acorde a los lineamientos de la Guía para la Administración del riesgo del DAFP V 6.0 de 2022.Se incluye el concepto de Mapa de Aseguramiento-Estructura Segunda Línea de Defensa, en los ítems:<ul style="list-style-type: none">9.2.1 Política Gobierno de Riesgos.10. Modelo de las 3 líneas de defensa. Figura 1.11.2.2.3 Servidores de media y alta gerencia (temas transversales).Anexo 1. Mapa de Aseguramiento - Estructura Segunda Línea de Defensa.	1, 3 y 4 9, 10, 11 y Anexo 1	Carlos Andrés Gutiérrez Basto
2.1	Cambio de forma	20/03/2025	<ul style="list-style-type: none">Se ajusta fuente, tamaño de letra y logotipo del documento acorde a lo establecido en el Manual de Identidad Corporativa UGPP vigente.	NA	Carlos Andrés Gutiérrez Basto

Antes de usar este documento revise en el listado maestro de documentos y verifique que esta es la última versión.

AP-FOR-008 V 2.0
Página 1 de 30



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

3.0	Cambio de fondo	30/11/2025	<ul style="list-style-type: none">• Se ajusta metodología acorde a los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V 7• Se incluyen las indicaciones para la gestión de riesgos en Proyectos de inversión pública y Proyectos críticos que afectan la operatividad y/o la continuidad del negocio.	NA	Carlos Andrés Gutiérrez Basto
-----	-----------------	------------	---	----	-------------------------------



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

TABLA DE CONTENIDO

1	INTRODUCCIÓN	4
2	OBJETIVOS DEL MANUAL	5
2.1	Objetivo General	5
3	MARCO NORMATIVO	5
4	ALCANCE	5
5	DEFINICIÓN DEL SISTEMA	6
6	OBJETIVO DEL SISTEMA	6
7	BENEFICIOS DEL SISTEMA	6
8	PRINCIPIOS DEL SISTEMA	7
9	POLÍTICA PARA LA ADMINISTRACIÓN DE RIESGOS	9
9.1	POLÍTICA GENERAL	9
9.2	POLÍTICAS ESPECÍFICAS	9
9.2.1	Política gobierno de riesgos	9
9.2.2	Política cultura de riesgos.....	10
9.2.3	Política de cumplimiento de normatividad interna y externa relacionadas con la administración de riesgos	11
9.2.4	Política de continuidad de negocio	12
9.2.5	Política Anticorrupción.....	12
9.2.6	Política de Seguridad de la Información.....	13
9.2.7	Política de conflicto de interés	13
10	MODELO DE LAS 3 LÍNEAS DE DEFENSA	13
11	ESTRUCTURA ORGANIZACIONAL DEL SISTEMA DE GESTIÓN DE RIESGOS ...	15
11.1	Perfiles, roles y funciones del sistema de gestión de riesgos corporativos	16
11.1.1	Línea Estratégica	16
11.2	Roles y responsabilidades de las tres líneas de defensa	17
11.2.1	Primera Línea de Defensa – Unidades de Negocio	17
11.2.2	Segunda Línea de Defensa – Función de Riesgos	22
11.2.3	Tercera Línea de Defensa	26
12	CARACTERIZACIÓN DEL PROCESO ADMINISTRAR RIESGOS CORPORATIVOS 28	
13	MECANISMOS DE COMUNICACIÓN	29
14	ANEXOS	30



MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS

AP-MAN-003

1 INTRODUCCIÓN

Cada vez cobra mayor importancia la necesidad de gestionar los crecientes riesgos a los que está expuesta una organización como un todo, razón por la cual se requiere realizar un manejo integral de los riesgos, que incluya dentro de la administración las diversas tipologías de riesgos tanto estratégicos como emergentes, generales de la gestión, para la integridad pública - SIGRIP, fiscales y de seguridad de la información.

Como parte del Sistema Integral del Riesgo se incorpora el Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP, el cual comprende el manejo de riesgos asociados a: soborno, fraude, inadecuada gestión del conflicto de intereses, corrupción, LA (Lavado de Activos)/FT (Financiación del Terrorismo) /FP (Financiación de la Proliferación de Armas de Destrucción Masiva), así como, la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas de gestión del riesgo.

El concepto de administración o gerencia del riesgo es muy amplio y se define como la identificación, evaluación, medición, control o transferencia de los riesgos a los que está expuesta una entidad y que pueden de alguna manera afectar la viabilidad de sus operaciones futuras.

En este sentido el Sistema de Gestión de Riesgos de la Entidad, es un conjunto de componentes que brindan las bases y disposiciones, para la aplicación sistemática de prácticas de gestión que permitan el establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos a los que está expuesta, entendiendo los riesgos como aquellos factores e influencias, internas y externas, que crean incertidumbre y afectan el logro de los objetivos de la Entidad.

	MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS	AP-MAN-003
---	--	-------------------

El Manual del Sistema de Gestión de Riesgos, es un documento orientador, que brinda una descripción de los elementos transversales del sistema y una guía que facilita el entendimiento de rol que juega cada uno los actores involucrados en la gestión del riesgo.

2 OBJETIVOS DEL MANUAL

2.1 Objetivo General

El presente documento tiene como objetivo relacionar y divulgar las políticas, los objetivos, la estructura organizacional, las responsabilidades y el proceso, aplicables en el desarrollo, implementación y seguimiento del Sistema de Gestión de Riesgo de la UGPP.

3 MARCO NORMATIVO

El Sistema de Gestión de Riesgos de la UGPP, responde a los siguientes lineamientos:

- Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG V.6 de Diciembre 2024 (establecido en el artículo 133 de la Ley 1753 de 2015) publicado por el Departamento Administrativo de la Función Pública
- Guía para la Gestión Integral del Riesgo en entidades públicas V7.

4 ALCANCE

Los conceptos descritos en este Manual aplican para la gestión de los riesgos estratégicos, emergentes, de gestión, integridad pública - SIGRIP, fiscales, de interrupción del negocio, de seguridad de la información y aquellos riesgos inherentes a los proyectos de inversión pública y proyectos críticos que afectan la operatividad y/o la continuidad del negocio.



MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS

AP-MAN-003

5 DEFINICIÓN DEL SISTEMA

El Sistema de Gestión de Riesgos (SGR) implementado en la UGPP es un conjunto de componentes que brindan las bases, lineamientos, disposiciones y estructura de gobierno, para aplicar de forma sistemática prácticas de gestión que permitan identificar, analizar, evaluar, tratar, monitorear y actualizar, los riesgos a los cuales está expuesta la Entidad.

El SGR le permite a la UGPP desarrollar, implementar y mejorar continuamente el marco de referencia para integrar la gestión del riesgo en los procesos globales de gobierno, planificación, políticas, valores y cultura de la organización, para aportar al cumplimiento de los objetivos estratégicos y a la consolidación de la excelencia operativa.

6 OBJETIVO DEL SISTEMA

Optimizar la gestión integral de los riesgos, contribuyendo al logro de las metas y objetivos de la Entidad y de sus procesos, fortaleciendo los criterios de estrategia y apetito de riesgo, gobierno de riesgos, cultura, evaluación y medición, gestión y monitoreo, reporte y perspectivas, datos y tecnología, en procura de la mejora continua del nivel de madurez del riesgo en la Entidad.

7 BENEFICIOS DEL SISTEMA

La implementación del Sistema de Gestión de Riesgos genera los siguientes beneficios y ventajas en todos los niveles de la Entidad y en la interrelación con sus grupos de interés:

- **Incrementa la capacidad de la Entidad para lograr sus objetivos** mediante la identificación y tratamiento preventivo de los riesgos potenciales.
- **Facilita a la alta Dirección la toma de decisiones basada en riesgos**, disminuyendo el nivel de incertidumbre.



MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS

AP-MAN-003

- **Potencia la eficacia de la Entidad** en la asignación y priorización de recursos hacia los procesos críticos que requieren mayor aseguramiento y monitoreo por su nivel de riesgo.
- **Incrementa la eficiencia de los procesos** al estar mejor asegurados por puntos de control y monitoreados sus riesgos por indicadores, disminuyendo reprocesos, costos de oportunidad y garantizando que las salidas cumplan con los requerimientos de oportunidad y calidad establecidos.
- **Incrementa la confianza de los grupos de interés en la Entidad** por la oportunidad, seguridad y transparencia percibida en los servicios ofrecidos.

8 PRINCIPIOS DEL SISTEMA

En el marco del Sistema de Gestión de Riesgos y teniendo como eje central la seguridad y transparencia de los procesos, los funcionarios de la UGPP basan su actuar en los siguientes principios:

- La gestión de riesgos genera y protege el valor: La gestión de los riesgos contribuye al logro de los objetivos estratégicos mediante el aseguramiento y mejoramiento de la eficiencia de todos sus procesos.
- La gestión de riesgos es una parte integral de todos los procesos de la Entidad: La gestión de riesgos es esencial para el adecuado funcionamiento, articulación e interrelación de los procesos, incluyendo aquellos que son gestionados y ejecutados por terceros.
- La gestión de riesgos es parte de la toma de decisiones: Los niveles de atribución, delegación y toma de decisiones en los procesos son basados en el nivel de exposición y apetito al riesgo.
- La gestión de riesgos aborda explícitamente la incertidumbre: El efecto de los riesgos sobre los objetivos estratégicos y de procesos es valorado según la probabilidad e impacto de su materialización, soportados en escenarios potenciales y/o eventos históricos.
- La gestión de riesgos es sistemática, estructurada y oportuna: La gestión de riesgos está fundamentada en las tres líneas de defensa (Dueños de procesos, Equipo de Riesgos, Auditoría interna) que



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

hacen parte del Gobierno de riesgos, esquema en el cual todos los funcionarios de los procesos contribuyen al aseguramiento y eficiencia de los procesos.

- La gestión de riesgos se basa en la mejor información disponible: Los análisis y estudios realizados para la gestión de riesgos son basados en datos históricos, eventos de riesgos y mejores prácticas disponibles para la identificación, medición, control y monitoreo de riesgos.
- La gestión de riesgos está adaptada a la organización: La gestión de riesgos abarca los diferentes tipos de riesgos: estratégicos, emergentes, gestión, integridad pública - SIGRIP, fiscales, interrupción del negocio, inherentes a los Proyectos de inversión pública y Proyectos críticos que afectan la operatividad y/o la continuidad del negocio y de seguridad de la información, de acuerdo con la naturaleza de la Entidad y el contexto externo e interno en los cuales está inmersa.
- La gestión de riesgos toma en consideración los factores humanos y culturales: La adecuada gestión de riesgos hace partícipes a todos los niveles de la organización (funcionarios, contratistas y proveedores) como un conjunto compenetrado en pro del fortalecimiento de la cultura de riesgos en la Entidad.
- La gestión de riesgos es transparente y aplica para todos: La gestión de riesgos presenta como su principal pilar el principio corporativo de la Transparencia, "Actuamos correctamente garantizando que todos nuestros comportamientos se ciñan a las normas legales vigentes, haciendo visible nuestro actuar de cara al ciudadano y al País".
- La gestión de riesgos es dinámica y adaptable a los cambios La gestión de riesgos como sistema está estructurado a partir de etapas de identificación, análisis, evaluación, tratamiento y monitoreo de riesgos que están interconectadas conformando un ciclo dinámico para su actualización en la medida que surjan o cambien los procesos, riesgos, controles, indicadores y planes de



MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS

AP-MAN-003

acción de acuerdo con el contexto interno o externo que afecte positiva o negativamente a la Entidad.

- La gestión de riesgos es continuamente monitoreada y mejorada. El monitoreo y evaluación como etapa clave en la gestión de riesgos se fundamenta en las tres líneas de defensa (Dueños de procesos, Equipo de Riesgos, Auditoría interna), las cuales se complementan y alinean entre sí, para la eficacia y eficiencia del seguimiento y evaluación de los diferentes elementos que hacen parte de la gestión de riesgos en los procesos.

9 POLÍTICA PARA LA ADMINISTRACIÓN DE RIESGOS

9.1 POLÍTICA GENERAL

La UGPP declara su compromiso de prevención y control de los riesgos identificados inherentes a su operación, basando la toma de decisiones para la planeación estratégica institucional y el ciclo de mejora y ejecución de los procesos, en la identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de dichos riesgos.

Para ello cuenta con la participación activa de sus colaboradores en la adecuada ejecución de las líneas de defensa en procesos, gestión de riesgos y auditoría, y se fomenta una cultura de la gestión integral del riesgo en todos los niveles de la Entidad lo cual incluye a los proveedores que soporten procesos.

9.2 POLÍTICAS ESPECÍFICAS

9.2.1 Política gobierno de riesgos

- a) El Equipo Directivo asume el compromiso de establecer una adecuada estructura organizacional en la Entidad que soporte el sistema de gestión integral de riesgos y valide los avances en el aseguramiento y nivel de madurez de este.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- b) El Equipo Directivo define el nivel de apetito al riesgo como “Bajo” y de cero tolerancia a los riesgos para la integridad pública, lineamiento con el cual se regirán todos los procesos, los cuales deberán garantizar un adecuado tratamiento de los riesgos residuales que se encuentren en niveles no admisibles.
- c) La gestión de riesgos está asegurada por tres líneas de defensa avaladas por la Dirección General de la entidad y las cuales están conformadas así:
- **Primera Línea de Defensa:** Directores Técnicos de las áreas, Subdirectores técnicos de las áreas, Coordinadores, líderes y ejecutores del proceso que ejercen autocontrol.
 - **Segunda Línea de Defensa:** Equipo de Trabajo de Gestión de Riesgos y el Grupo Interno de Trabajo de Seguridad de la información adscritos a la Dirección de Seguimiento y Mejoramiento de Procesos. Igualmente, hacen parte de la segunda línea de defensa los servidores de media y alta gerencia de las áreas de la Entidad que consolidan y analizan información sobre temas transversales y clave para la Entidad, que sirven de base para la toma de decisiones y acciones preventivas necesarias para evitar la materialización de riesgo.
 - **Tercera Línea de Defensa:** Oficina de Control Interno.
- d) Cada Director de área, con el acompañamiento metodológico del Equipo de Trabajo de Gestión de Riesgos de la Dirección de Seguimiento y Mejoramiento de Procesos, asume la responsabilidad de evaluar y hacer seguimiento de la evolución de la gestión integral de los riesgos inherentes a sus procesos en cuanto a la efectividad de los controles, acciones de tratamiento y toma de decisiones basadas en los niveles de alerta de los Indicadores Clave de Riesgo (KRI).

9.2.2 Política cultura de riesgos

- a) La Dirección General genera las directrices y dispone de los recursos necesarios para el impulso, fortalecimiento y



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

mantenimiento de la cultura de gestión de riesgos al interior de todos los procesos de la entidad, dando los lineamientos para establecer las herramientas que deben ser implementadas para la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los diferentes tipos de riesgos a los que está expuesta.

- b) El equipo de trabajo de Gestión de Riesgos impulsa la gestión unificada de los diferentes tipos de riesgos a nivel de toda la Entidad y promueve las directrices, herramientas y metodologías para la articulación de los diferentes elementos de administración de riesgos en la cultura corporativa propendiendo por el aseguramiento y control de los procesos.
- c) En concordancia con el fortalecimiento de la cultura de riesgos todos los funcionarios de la Entidad podrán ser evaluados periódicamente según el grado de cumplimiento de los elementos de gestión de riesgos en los procesos, por medio de indicadores vinculados directamente a los compromisos individuales. En este sentido, en los "Acuerdos de Gestión" que se fijen con el Equipo Directivo y en los "Compromisos Laborales y Comportamentales" que se definan con los demás funcionarios, se pueden establecer compromisos medibles y alcanzables relacionados con la gestión de riesgos.

9.2.3 Política de cumplimiento de normatividad interna y externa relacionadas con la administración de riesgos

La Dirección General y el Equipo Directivo de la UGPP establecen las políticas, normas, lineamientos y directrices para la adecuada administración de los riesgos, para el aseguramiento de los procesos y la consecución de los objetivos estratégicos y de procesos tomando como referencia los diferentes marcos y estándares normativos que enmarcan a los sistemas de administración de riesgos, entre estos: Estatuto anticorrupción ley 1474 de 2011, COSO ERM, Modelo Integrado de Planeación y Gestión (MIPG), Código de Integridad y la Guía para la Gestión Integral del Riesgo en Entidades Públicas (DAFP,

	MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS	AP-MAN-003
---	--	-------------------

Secretaría de Transparencia de la Presidencia de la República, MinTIC, MinSalud, SuperSalud).

Lo dictaminado en materia de riesgos es de obligatorio cumplimiento por parte de todos los funcionarios, contratistas y proveedores de la UGPP; su incumplimiento acarreará sanciones disciplinarias para los primeros de acuerdo con lo definido por Control Interno Disciplinario y terminación de contrato o pago de indemnizaciones para los segundos.

9.2.4 Política de continuidad de negocio

La Entidad declara su compromiso con la construcción y mantenimiento de un Sistema de Continuidad de Negocio, en el cual se consignarán los protocolos, así como las medidas preventivas y reactivas para poder enfrentar cualquier evento interno o externo, que, por su naturaleza y nivel de impacto, pueda dar lugar a una interrupción parcial y/o total del negocio, que comprometa la continuidad de los procesos críticos y de atención al ciudadano. Este plan tendrá como objetivo salvaguardar los intereses de las partes interesadas, la gobernabilidad, la reputación y las actividades de creación de valor.

Una vez definido el plan, será de obligatorio cumplimiento por parte de los funcionarios, contratistas y proveedores que trabajen en, o por fuera de las instalaciones de la Entidad, los lineamientos que allí se dispongan, así como la participación en los simulacros de continuidad cuando sean requeridos.

9.2.5 Política Anticorrupción

La UGPP es una Entidad totalmente alineada con el Gobierno Nacional frente a la lucha contra la corrupción. Por tanto, sus servidores públicos, contratistas y proveedores deben ser personas íntegras en su actuar y proceder, honestas y transparentes, su posición debe ser abiertamente en contra de cualquier conducta irregular, y su actitud,

	MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS	AP-MAN-003
---	--	-------------------

la de denunciar ante las autoridades correspondientes cuando se evidencie alguna de ellas.

9.2.6 Política de Seguridad de la Información

Ver la política corporativa de Seguridad de la Información TI-PIT-001.

9.2.7 Política de conflicto de interés

Los funcionarios de la UGPP deberán declararse impedidos para actuar en un asunto cuando se tenga interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil.

Igualmente deberá declararse impedido cuando el interés general, propio de la función pública, entre en conflicto con su interés particular y directo.

La política de conflicto de interés se encuentra alineada con el Código de Ética, el cual contiene las directrices comportamentales aplicables a todos los funcionarios de la Entidad.

10 MODELO DE LAS 3 LÍNEAS DE DEFENSA

El modelo de las tres líneas de defensa para la gestión de riesgos busca asegurar que las responsabilidades relacionadas con la gestión de riesgos y el control estén distribuidas en distintas áreas y divisiones y se ejerzan de forma coordinada. Es un esquema que establece los roles y responsabilidades de todos los actores en la gestión y control del riesgo en la Entidad; proporcionando una estructura de aseguramiento de la gestión, previniendo la materialización de los riesgos en todos sus ámbitos

	MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS	AP-MAN-003
---	--	-------------------

El modelo de las Tres Líneas de Defensa distingue tres grupos (o líneas) que participan en una efectiva gestión de riesgos:

- Las funciones que son propietarias de los riesgos y los gestionan.
- Las funciones que supervisan los riesgos.
- Las funciones que proporcionan aseguramiento independiente.

En este modelo de control, las unidades de negocio son la primera línea de defensa en la gestión de riesgos; las funciones de supervisión de riesgos, controles y cumplimiento establecidas por la administración son la segunda línea de defensa; y el aseguramiento independiente es la tercera línea.

Para el caso particular de la segunda línea de defensa, la UGPP ha construido un Mapa de Aseguramiento el cual es un esquema visual que muestra la estructura de esta línea, permitiendo coordinar los diferentes servicios de aseguramiento y visualizar esfuerzos en común, respecto a la gestión de los riesgos clave en los procesos de la Entidad, mostrando el nivel de confianza de dichos servicios proporcionados por los diversos proveedores. En el Anexo 1 se presenta este Mapa de Aseguramiento – Estructura Segunda Línea de Defensa.

Cada una de estas "líneas" juega un papel distinto dentro del marco amplio de gobernabilidad de la Entidad tal como se representa en la siguiente figura.

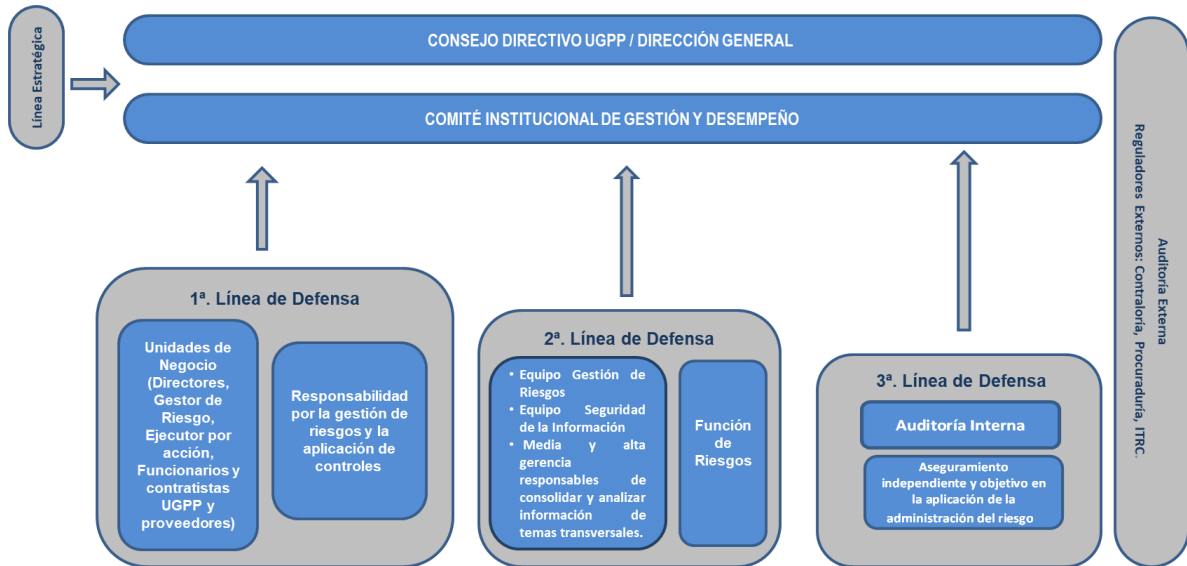


Figura 1. Modelo tres líneas de defensa para una efectiva gestión de riesgos y control

Basado en: [Publicación de Función Pública sobre las tres líneas de defensa en gestión de riesgos](#)

11 ESTRUCTURA ORGANIZACIONAL DEL SISTEMA DE GESTIÓN DE RIESGOS

La UGPP cuenta con una estructura de gobierno para la gestión de riesgos enfocada en tres líneas de defensa, este modelo de defensa va dirigido a la alineación del aseguramiento del gobierno corporativo de los riesgos, donde se reconoce la existencia de diferentes órganos de gestión de riesgos y controles y propone una asignación de funciones, roles y responsabilidades en aspectos tales como la titularidad del riesgo, el control del riesgo y la garantía del control.

Todos estos equipos deberán trabajar de una manera coordinada y conjunta enfocados a proteger a la UGPP contra los riesgos, ser capaces de crear una asignación de roles y responsabilidades suficientemente claros, de modo que cada grupo de profesionales de riesgo y control entienda los límites de sus responsabilidades y cómo encaja su rol en la estructura general de riesgo y control de la



MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS

AP-MAN-003

Entidad, para tener una visión completa de la gestión del riesgo que elimine las brechas, se mejoren los mecanismos de comunicación y retroalimentación y se mantenga la relación necesaria entre las líneas de defensa.

La Dirección de la UGPP, proveerá los recursos necesarios para implementar y mantener en funcionamiento el Sistema de Gestión de Riesgos Corporativos de forma efectiva y eficiente, con una estructura organizacional que permita el funcionamiento y administración integral de los riesgos.

Las responsabilidades de la gestión integral de riesgos se establecen desde la Alta Dirección, hasta cada una de las áreas de la UGPP quienes son responsables de administrar el riesgo acorde con las metodologías y herramientas definidas.

11.1 Perfiles, roles y funciones del sistema de gestión de riesgos corporativos

11.1.1 Línea Estratégica

La línea estratégica define el marco general para la gestión del riesgo y el control, y supervisa su cumplimiento; en la Entidad se encuentra compuesto por la Alta Dirección (Consejo Directivo y Dirección General) y el Comité Institucional de Gestión y Desempeño.

Para este fin ejecuta las siguientes funciones:

- Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la Entidad.
- Establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la Entidad.
- Evaluar y dar línea sobre la administración de los riesgos en la Entidad.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Realimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles.
- Revisar los cambios en el “Direccionamiento estratégico” y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Hacer seguimiento en el Comité Institucional de Gestión y Desempeño a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno.
- Revisar el cumplimiento a los objetivos institucionales e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando.
- Hacer seguimiento y pronunciarse periódicamente sobre el perfil de riesgo inherente y residual de la Entidad, incluyendo los riesgos para la Integridad Pública – SIGRIP y de acuerdo con la tolerancia al riesgo establecida.

11.2 Roles y responsabilidades de las tres líneas de defensa

11.2.1 Primera Línea de Defensa – Unidades de Negocio

La primera línea de defensa desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

11.2.1.1 Directores Técnicos y Líderes de Proceso

Su rol principal es diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la Entidad.

Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la Entidad y emprender las acciones de mejoramiento para su logro.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

Esta primera línea de defensa tiene a cargo las siguientes funciones y responsabilidades:

- Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales.
- Definir, implementar y revisar la adecuada ejecución de los controles establecidos para la mitigación de los riesgos asociados a los procesos a su cargo.
- Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. Igualmente, implementar procesos para identificar, disuadir y detectar fraudes; y revisar la exposición de la Entidad al fraude con el auditor interno de la Entidad.
- 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 sus procesos, para la actualización del mapa de riesgos de su proceso.
- Revisar que las actividades de control de sus procesos se encuentren actualizadas y documentadas.
- 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.
- Revisar y reportar al Equipo de Gestión de Riesgos, los eventos de riesgos que se han materializado en la Entidad, incluyendo los riesgos de para la integridad pública – SIGRIP y fiscales, identificando las causas que dieron origen a esos eventos.
- 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 y lograr el cumplimiento de los objetivos.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
- Asegurarse de implementar la metodología de gestión de riesgos para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.
- Identificar los riesgos asociados en cada una de las fases de los Proyectos de inversión pública y Proyectos críticos que afectan la operatividad y/o la continuidad del negocio, establecer controles y realizar seguimiento para verificar el cumplimiento de los mismos acorde a la periodicidad definida y en el evento de materializarse un riesgo tomar las acciones o decisiones oportuna para disminuir el impacto frente a los objetivos del Proyecto.

11.2.1.2 Gestor de Riesgos

Los Gestores de Riesgos son funcionarios pertenecientes a cada área que, por su conocimiento amplio de los procesos, son designados formalmente por el dueño de proceso para trabajar en conjunto con el Equipo de Gestión de Riesgos en la implementación, seguimiento y mejora de los diferentes elementos de la administración de los riesgos en cada uno de los procesos.

Dentro de las principales funciones se encuentran:

- Servir de contacto primario con el Equipo de Gestión de Riesgos de la Dirección de Seguimiento y Mejoramiento de Procesos, para el sostenimiento de la gestión de riesgos en su proceso.
- Impulsar y promover el Sistema de Gestión de Riesgos en su proceso.
- Colaborar en la identificación de los riesgos a que se ve expuesta la Entidad, teniendo en cuenta los factores de riesgo: Ejecución y administración de procesos, Transacción u Operación (aplica para LA/FT/FP, Talento Humano, Tecnología, Infraestructura, Evento externo).



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Liderar la implementación de controles con el fin de disminuir la probabilidad de ocurrencia de los riesgos a los que está expuesto su proceso y mitigar su impacto en caso de que dichos riesgos se materialicen.
- Monitorear el comportamiento de los riesgos de su proceso y registrar, cuantificar y reportar al Equipo de Gestión de Riesgos, cualquier evento de riesgo materializado inmediatamente éste ocurra.
- Velar porque el registro de eventos de riesgos cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.
- Participar en la definición de los Indicadores Clave de Riesgo (Key Risk Indicator - KRI) y de los Indicadores Clave de Control (Key Control Indicator - KCI); monitorearlos, analizarlos y reportar los resultados de su medición periódicamente en las herramientas establecidas para este fin.
- Asegurar la generación y seguimiento de los planes de acción necesarios para la gestión de los riesgos y la mitigación de los eventos de materialización, e informar periódicamente su avance al Equipo de Gestión de Riesgos.
- Notificar a la Dirección de Seguimiento y Mejoramiento de Procesos y al Equipo de Riesgos, los cambios que se hayan realizado a los procesos y/o controles producto de la gestión de los riesgos, para su oportuna actualización.
- Asegurar que la información correspondiente a la gestión de riesgos de su proceso esté actualizada en los formatos definidos o cualquier sistema de información corporativo vigente.
- Servir de facilitador del cambio cultural de los funcionarios de su proceso, contratistas y proveedores frente a la Gestión Integral de riesgos.
- Aplicar los instrumentos, metodologías y/o procedimientos definidos para la gestión y administración efectiva de sus riesgos.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Acompañar y retroalimentar el análisis de la gestión de riesgos de su proceso, a partir de la información resultante de la gestión de riesgos de cada periodo.
- Asistir a las citaciones para Gestores de Riesgos, talleres y demás reuniones programadas por la Dirección de Seguimiento y Mejoramiento de Procesos en cabeza del Equipo de Gestión de Riesgos.

11.2.1.3 Ejecutor por Acción

Es el funcionario responsable de la formulación y ejecución de los planes de acción generados con el fin de mitigar la materialización de un riesgo.

Entre sus funciones se encuentran:

- Asegurar la oportuna ejecución de las acciones de tratamiento de riesgos a su cargo, conservando las evidencias de su aplicación en los repositorios de información que la Subdirección y /o Coordinación definan para este propósito.
- Informar al Dueño de Proceso y al Gestor de Riesgos, sobre los avances, barreras y oportunidades identificadas durante la ejecución de las acciones de tratamiento.

11.2.1.4 Funcionarios de la UGPP

Todos los servidores y colaboradores de La UGPP deben:

- Participar en la implementación del Sistema de Gestión de Riesgos Corporativos.
- Aplicar el Código de Ética de la Entidad, sus Principios y Valores, al Sistema de Gestión de Riesgos Corporativos.
- Aplicar lo establecido en el Manual del Sistema de Gestión de Riesgos Corporativos, y sus anexos.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Reportar cualquier problema que se presente en la ejecución de sus actividades, en cumplimiento de normas o posibles faltas al Código de Ética.
- Ejecutar las actividades asignadas en el Manual de Funciones y caracterizaciones de procesos, tomando las acciones necesarias para el control de riesgos.
- Reportar los nuevos riesgos que identifique, incidentes o riesgos materializados y eventos de riesgo ocurridos o conocidos en el desarrollo de sus actividades, de acuerdo con la metodología definida y las herramientas establecidas para este fin.
- Informar al Equipo de Gestión de Riesgos, sobre cualquier señal de alerta que evidencien en el desarrollo de sus funciones y proponer nuevos mecanismos de control.
- Administrar los riesgos generados en los procesos a su cargo o en los que participa, mediante la implementación Sistema de Gestión de Riesgos Corporativos.
- Informar sobre cualquier operación inusual de la que tengan conocimiento.
- Atender los requerimientos y solicitudes que realice el Equipo de Gestión de Riesgos, y colaborar para el buen funcionamiento del Sistema de Gestión de Riesgos Corporativos.
- Participar activamente en los programas de formación del Sistema de Gestión de Riesgos establecidos por la Entidad

11.2.2 Segunda Línea de Defensa – Función de Riesgos

Los equipos que conforman la segunda línea de defensa cuentan con un rol transversal a toda la Entidad; sus procesos, operaciones y responsabilidades están enfocadas a facilitar, promover y vigilar que las prácticas y métodos definidos para la gestión de los riesgos sean implementadas y seguidas de manera efectiva por la primera línea de defensa.

Este rol es ejecutado por el Equipo de Gestión de Riesgos, el Equipo de Seguridad de la Información y por funcionarios que ocupan cargos

	MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS	AP-MAN-003
---	--	-------------------

de media y alta gerencia responsables de consolidar y analizar información de temas transversales que son clave para la Entidad.

11.2.2.1 Equipo de Gestión de Riesgos

Su rol principal es monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo. Así mismo, asiste 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 de sus procesos a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

Dentro de las responsabilidades específicas del Equipo de Gestión de Riesgos se encuentran:

- Proponer la estrategia y lineamientos para implementar el sistema de gestión de riesgos en la UGPP.
- Diseñar y proporcionar el marco metodológico para la gestión de riesgos en la Entidad.
- Definir las metodologías específicas y los instrumentos necesarios para que la Entidad administre efectivamente sus riesgos.
- Vigilar que el marco metodológico, las metodologías específicas y los instrumentos de gestión de riesgos se apliquen de manera efectiva en la Entidad.
- Desarrollar, acompañar y promover en la Entidad la consolidación de una cultura en materia de gestión de riesgos.
- Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada.
- Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude.
- Consolidar los seguimientos a los mapas de riesgo.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Elaborar informes consolidados para las diversas partes interesadas.
- Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar.
- 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 los procesos, con el fin de solicitar y apoyar en la actualización de los mapas de riesgos.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.
- Revisar el nivel de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del nivel de riesgo de la Entidad.
- Hacer seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos para asegurar que se encuentren documentadas y actualizadas en los procedimientos.
- 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 de los objetivos.

11.2.2.2 Equipo de Seguridad de la Información

El equipo de Seguridad de la Información es responsable de la seguridad de todos los activos de la información identificados en la Entidad, apoya y acompaña a las diferentes líneas de defensa tanto para el reporte, como para la gestión y el tratamiento de estos riesgos de seguridad de la información.

Dentro de sus funciones se encuentran:



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Participar en el diseño, implementación y mantenimiento de controles efectivos en materia de seguridad de la información, de acuerdo con los procedimientos definidos.
- Gestionar el proceso de administración de riesgos de seguridad de la información monitoreando la efectividad de los controles y proponiendo mejoras.
- Identificar, valorar, tratar, comunicar, monitorear y revisar los riesgos de seguridad de la información, que pueden impactar la confidencialidad, integridad o disponibilidad de los activos de información críticos de la Entidad.

11.2.2.3 Servidores de media y alta gerencia (temas transversales)

Los servidores de media y alta gerencia que poseen información sobre temas transversales de la Entidad, son responsables de generar reportes y presentarlos a la alta Dirección de tal forma que se facilite el aseguramiento (seguimiento, monitoreo, evaluación). El aseguramiento se realiza de manera transversal en las áreas o procesos de la Entidad donde se gestiona el aspecto a asegurar, consolidando y analizando la información reportada por la 1ª primera línea de defensa, de tal manera que genere valor a la alta gerencia para la toma de decisiones.

Dentro de sus funciones se encuentran:

- Efectuar seguimiento al desarrollo del tema transversal en la Entidad de conformidad con los lineamientos previamente establecidos, retroalimentando y generando alertas a la primera línea de defensa. –
- Evaluar el tema transversal de manera consolidada y estratégica, generando información y alertas a la línea estratégica para la toma de decisiones.

	MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS	AP-MAN-003
---	--	-------------------

11.2.3 Tercera Línea de Defensa

11.2.3.1 Oficina de Control Interno

Esta línea de defensa proporciona información sobre la efectividad del Sistema de Control Interno (SCI), a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

Su rol principal es proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del SCI. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del SCI.

Así mismo, provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso.

La tercera línea de defensa se encuentra representada por el equipo de Control Interno de la UGPP y es la encargada de las siguientes funciones:

- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.
- Proporcionar seguridad razonable con respecto al diseño e implementación de políticas, procedimientos y otros controles.
- Evaluar si los procesos de gobierno de TI de la Entidad apoyan las estrategias y los objetivos de la entidad.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

- Proporcionar información sobre la eficiencia, efectividad e integridad de los controles tecnológicos y, según sea apropiado, puede recomendar mejoras a las actividades de control específicas.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de para la integridad pública – SIGRIP y fiscales.
- 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.
- Revisar el nivel de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del nivel establecido como apetito de riesgo de la Entidad o que su calificación de impacto o probabilidad del riesgo no sea coherente con los resultados de las auditorías realizadas.
- 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 subprocesos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna mitigando la causa raíz del problema, propendiendo por no repetición de hallazgos o materialización de riesgos.
- Realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la Entidad, catalogándola como una unidad auditable más, dentro de su universo de auditoría, y por lo tanto debe dar a conocer a toda la Entidad el Plan Anual de Auditorias basado en riesgos, y los resultados de la evaluación de la gestión del riesgo.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

**11.2.1.2 Auditores externos, reguladores y otros entes
externos**

Más allá de las 3 líneas de defensa existen algunos organismos externos que contribuyen a la estructura de gobierno, gestión del riesgo y control interno, estos son:

- Contraloría General de la República.
- Procuraduría General de la Nación.
- Inspector de Tributos, Rentas y Contribuciones ITRC.

La auditoría externa ofrece garantías al Consejo Directivo y a la Alta Dirección, con respecto a la fidelidad e integridad de los estados financieros y de los sistemas de administración de riesgos existentes.

Los entes reguladores externos, establecen requerimientos normativos y legales con la intención de implementar controles, asegurar que se gestionen determinados aspectos de riesgos y fortalecer los mecanismos de control interno de los supervisados.

Igualmente, estos reguladores pueden llevar a cabo evaluaciones totales o parciales de la implementación y cumplimiento de las normas y requerimientos impartidos, proporcionando un nivel más de aseguramiento de gestión para las partes interesadas y la Alta Dirección.

**12 CARACTERIZACIÓN DEL PROCESO ADMINISTRAR RIESGOS
CORPORATIVOS**

Bajo los lineamientos del Sistema Integrado de Gestión de la Entidad, se tiene establecido el Proceso Administrar Riesgos Corporativos, el cual tiene por objetivo identificar, evaluar, tratar, hacer seguimiento y comunicar los riesgos asociados a los objetivos estratégicos y a los objetivos de los procesos de la organización, con el fin de proporcionar a la administración un aseguramiento razonable con respecto al logro de estos.



**MANUAL SISTEMA DE GESTIÓN
DE RIESGOS CORPORATIVOS**

AP-MAN-003

La responsabilidad por el liderazgo en la implementación del Proceso Administrar Riesgos Corporativos se encuentra a cargo de la Dirección de Seguimiento y Mejoramiento de Procesos, a través del Equipo de Gestión de Riesgos.

El alcance de este proceso inicia con la revisión de la estrategia organizacional o del proceso sobre el cual se van a identificar los riesgos, y termina con la generación de los informes de seguimiento a los planes de manejo diseñados y la divulgación de los mapas de riesgos.

Los demás detalles acerca de este proceso se encuentran en el documento: AP-PRO-003 Caracterización Proceso Administrar Riesgos Corporativos, que hace parte del Macroproceso Aseguramiento de Procesos.

13 MECANISMOS DE COMUNICACIÓN

Con el propósito de mantener permanentemente informadas a todas las partes interesadas en relación con los avances y novedades del Sistema de Gestión de Riesgos y fortalecer la cultura de Gestión del Riesgo se han definido los siguientes mecanismos de comunicación:

- El Equipo de Gestión de Riesgos de la Dirección de Seguimiento y Mejoramiento de Procesos, a través de sesiones presenciales y virtuales informa permanentemente al Comité Directivo y al Consejo Directivo el desarrollo del Sistema de Gestión de Riesgos exponiendo y sustentando los temas que requieren de su aprobación.
- A través del Site del Sistema Integrado de Gestión se divulga a todos los funcionarios de la Entidad, la información y los documentos propios del Sistema de Gestión de Riesgos.
- Con el apoyo de la Oficina de Comunicaciones de la Entidad a través del correo electrónico se informa a todos los funcionarios de

	MANUAL SISTEMA DE GESTIÓN DE RIESGOS CORPORATIVOS	AP-MAN-003
---	--	-------------------

la Entidad las noticias y novedades relacionadas con el Sistema de Gestión de Riesgos.

14 ANEXOS

Anexo 1. Mapa de Aseguramiento – Estructura Segunda Línea de Defensa.