SISTEMA DE GESTIÓN DE RIESGOS

MARTHA CECILIA CASTRILLÓN SUÁREZ

Gerente ESE Metrosalud

Oficina Asesora Planeación y Desarrollo Organizacional

30/06/2021

Versión [02]

Alcaldía de Medellín

PLATAFORMA ESTRATÉGICA Y CONTENIDO INSTITUCIONAL

La empresa Metrosalud es una Empresa Social del Estado del orden Municipal, constituida según Decreto 752 del 23 de junio de 1994 y mediante Decreto 883 de 2015; adquiriendo la categoría de entidad descentralizada con personería jurídica, patrimonio propio y autonomía administrativa. La E.S.E Metrosalud surgida a la luz de la ley 100 de 1993 y reglamentada por las leyes 1122 del 2007 y 1438 del 2011 conserva en el tiempo su unidad de empresa; y después de su creación en 1994, comenzó un proceso de adaptación a la nueva normatividad; logrando durante este tiempo importantes desarrollos que la han catalogado como la red de servicios de salud más grande de Colombia.

La E.S.E Metrosalud tiene una plataforma estratégica que le permite definir pautas importantes para la gestión como son: Misión, Visión, Ventaja competitiva, Promesa de valor, Objetivos corporativos, Competencias corporativas. Ver enlace http://www.metrosalud.gov.co/metrosalud/institucional

Principios y valores corporativos. Ver enlace:
http://www.metrosalud.gov.co/metrosalud/principios-y-valores

Organigrama institucional. Ver enlace:

http://www.metrosalud.gov.co/metrosalud/organigrama

Mapa de procesos. Ver enlace:

http://www.metrosalud.gov.co/metrosalud/estructura-de-procesos

Deberes y Derechos de los usuarios. Ver enlace:

http://www.metrosalud.gov.co/usuarios/derechos-y-deberes

Reseña Histórica. Ver enlace:

http://www.metrosalud.gov.co/metrosalud/historia

1. INTRODUCCIÓN

Las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que hacen incierto si lograrán sus objetivos. El "Efecto de la incertidumbre sobre los objetivos" se conoce como riesgo. NTC ISO 31000

La gestión del riesgo, como elemento de gestión:

- Ayuda al conocimiento y mejoramiento de la entidad, contribuye a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad.
- Es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas. Es parte de la GOBERNANZA y el LIDERAZGO y es fundamental en la manera en que se gestiona la organización en todos sus niveles, contribuyendo a la mejora de los sistemas de gestión.
- Es parte de todas las actividades de la organización y de su interacción con las partes interesadas, considera el contexto externo e interno, incluido el comportamiento humano y factores culturales.

Para su implementación es necesario que la organización haga un análisis de las estrategias, la formulación de objetivos y la implementación de esos objetivos en la toma de decisiones cotidiana, lo que permitirá una identificación del riesgo adecuada a sus necesidades, con un enfoque preventivo que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a sus usuarios aspectos fundamentales frente a la generación de valor público, eje fundamental en el quehacer de todas las organizaciones públicas.

Los contenidos de este sistema están debidamente articulados con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción, seguridad de la información y Sistema de Prevención de Lavado de Activos y Financiación del Terrorismo SARLAFT.

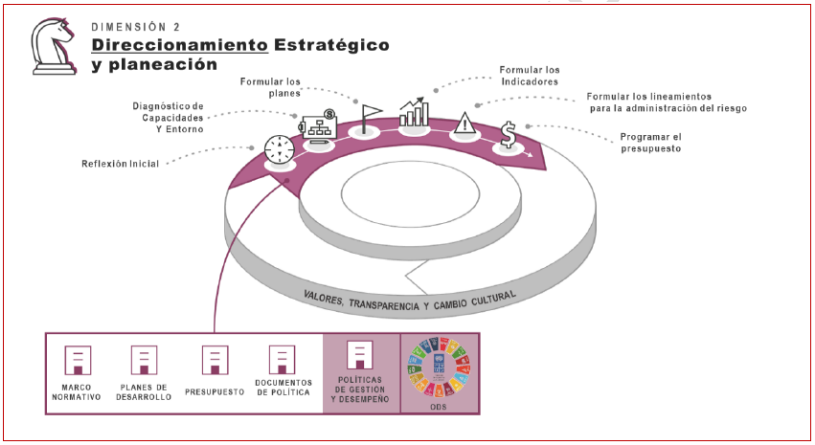
El estado colombiano, mediante Ley 87 de 1993 establece normas para el ejercicio del control interno en la entidades, como una herramienta de control que permite la implementación y fortalecimiento de los sistemas de control interno, asegurando razonablemente el cumplimiento de sus objetivos y a través del Decreto 1537 de 2001 que la reglamenta, orienta el establecimiento y aplicación de la política de administración de 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, con 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, 2021, p. 8) y así mismo da los lineamientos para la implementación de la gestión de riesgos en las entidades del sector público.

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.

Como se ilustra en las imágenes, la "Gestión del Riesgo" es uno de los componentes del Modelo Integrado de Gestión y Planeación MIPG, contenido en la Dimensión 2 de Direccionamiento Estratégico y Planeación y en la Dimensión 7 de Control Interno.

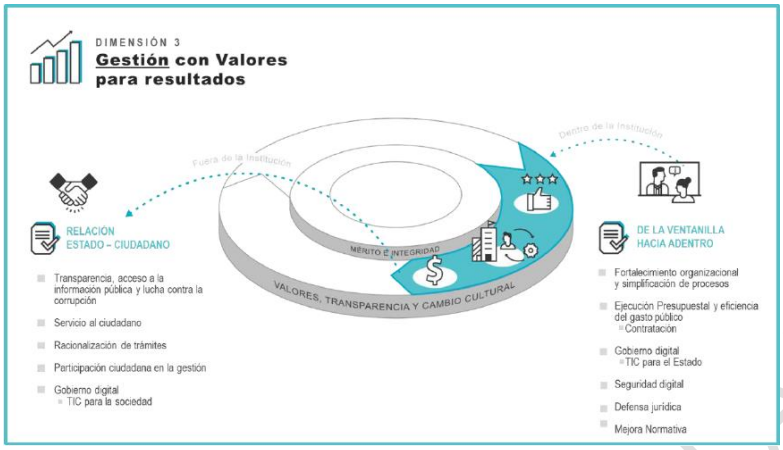
En la Dimensión 2 se orienta la formulación de los lineamientos para la gestión de riesgos - Política de administración de riesgos, que incluye los factores de riesgo (Análisis Interno y Externo), la planeación estratégica de la entidad y el Plan Anticorrupción y Atención al ciudadano



Dimensión 2 MIPG, Direccionamiento Estratégico y Planeación 2021. DAFP

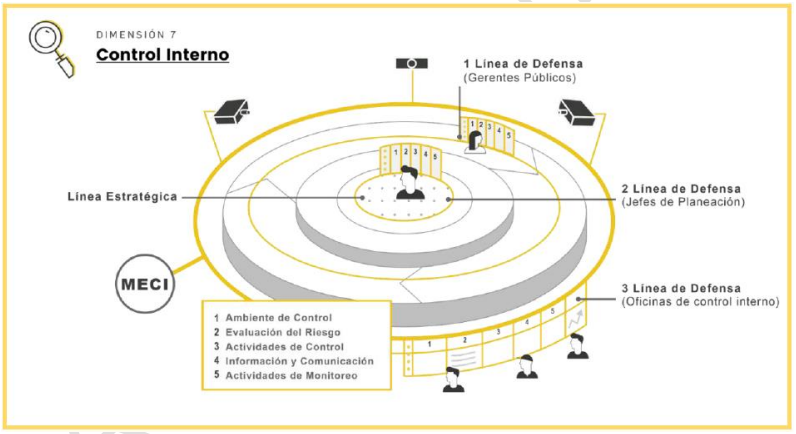
En la Dimensión 3 Gestión con Valores para el Resultado, se definen los siguientes aspectos, que se articulan con la gestión de riesgos:

- Estructura de Procesos, Procedimientos, Políticas, entre otras herramientas, temas concebidos en cascada desde la misión, visión y objetivos estratégicos de la entidad.
- Instrumentos y herramientas relacionadas con las Tecnologías de la Información y las Comunicaciones para la mejora de los procesos.



Dimensión 3 MIPG Valores con Resultados 2021. DAFP

En la Dimensión 7 Control Interno, se dan los lineamientos para asegurar la gestión del riesgo en las entidades, incluyendo riesgos de fraude y corrupción, a través de las tres líneas de defensa y el diseño e implementación de actividades de control del riesgo.



Dimensión 7 MIPG, Control Interno 2021. DAFP

De otro lado, la NTC - ISO 31000 brinda los principios y directrices genéricas sobre la gestión del riesgo, y como parte de la implementación de buenas práctica en el Sistema Integrado de Gestión, la ESE Metrosalud toma como insumo de su gestión de riesgos esta norma, alineándola con las directrices de la Función Pública DAFP.

Además de lo anterior, y como parte de la gestión de riesgos de la ESE Metrosalud, deben tenerse en cuenta los objetivos corporativos y lineamientos normativos que aplican a la empresa, de manera que se trabajen de forma conjunta sus elementos, en el desarrollo metodológico, los cuales se detallan en el Marco Normativo.

Este documento suministra los lineamientos para la gestión del riesgo, de una manera sistemática, secuencial y lógica, a través de una serie de pasos o etapas, que van desde la definición del "contexto del riesgo" y del "contexto organizacional" hasta el "tratamiento del riesgo" y monitoreo a la gestión de riesgos.

2. OBJETIVO

Este documento establece los lineamientos generales y acciones para la gestión del riesgo en la ESE Metrosalud, en relación con los riesgos organizacionales y riesgos por proceso (incluyendo los riesgos de seguridad del paciente derivados del proceso de atención en salud riesgos de corrupción, riesgos de Lavado de Activos y Financiación del Terrorismo LA/FT, riesgo en seguridad digital, y riesgos de Seguridad y Salud en el Trabajo SG- SST), procurando la uniformidad en su aplicación, con el fin de:

- Incrementar la capacidad de la entidad para alcanzar sus objetivos.
- Involucrar y comprometer a todos los servidores en la búsqueda de acciones para prevenir y administrar los riesgos, fortaleciendo la cultura del autocontrol.
- Proteger los recursos de la institución y del Estado y minimizar las pérdidas
- Establecer una base confiable para la toma de decisiones y la planeación.
- Cumplir los requisitos legales y reglamentarios pertinentes y evitar sanciones
- Mejorar la eficacia y eficiencia operativa.
- Incrementar el desempeño de la salud y la seguridad, así como la seguridad ambiental.
- Fomentar el aprendizaje organizacional y el mejoramiento de los procesos

3. LINEAMIENTOS DE POLÍTICA

La ESE Metrosalud cuenta con una **Política de Gestión de Riesgos** publicada en el SGI Almera, que incluye lineamientos frente a la gestión de riesgos de corrupción, de Lavado de Activo y Financiación del Terrrorismo LA/FT y seguridad digital, contenidos en el marco normativo aplicable.

4. ALCANCE

La gestión del riesgo es el término aplicado a un método lógico y sistemático, iterativo, compuesto por una serie de pasos que, si se ejecutan secuencialmente, permiten la mejora continua en la toma de decisiones.

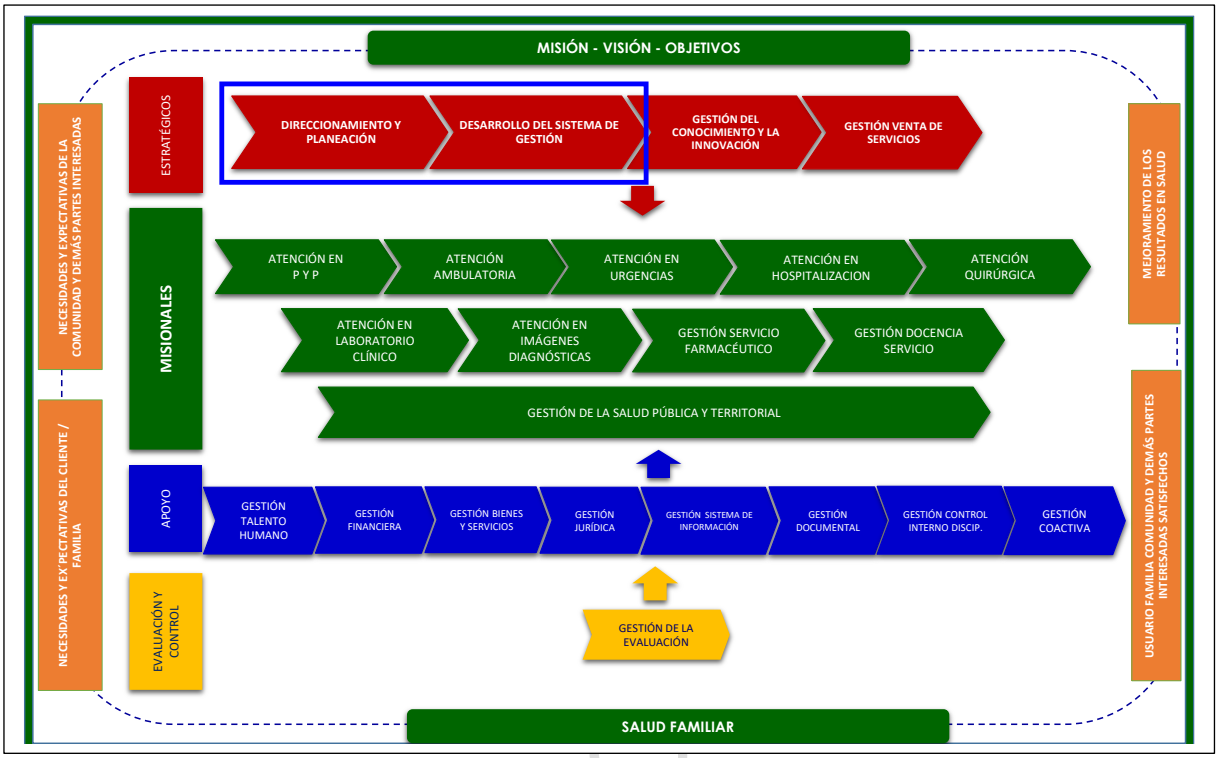
Este sistema y la metodología aquí descrita aplican a toda la organización, a sus objetivos estratégicos, sistemas, modelos, planes, programas, proyectos y procesos, incluidas aquellas actividades que son realizadas por un tercero a través de un proceso contractual.

Fundamentalmente hace parte del trabajo del día a día a través de la ejecución de los procesos y procedimientos, en todas las dependencias, tanto asistenciales como administrativas.

5. CONTEXTO DE METROSALUD FRENTE AL SISTEMA DE GESTIÓN DE RIESGOS

La ESE Metrosalud, desde el año 2012, adopta y define el Sistema de Administración de Riesgos, SAR, el cual ha sido ajustado en varias oportunidades acorde con la dinámica institucional y normas vigentes en el asunto. A partir de abril de 2017 la gestión de riesgos y su seguimiento se asigna al Comité de Coordinación de Control Interno, el cual incluye en su Plan de Trabajo las acciones pertinentes para ello.

En 2018 a través del Acuerdo 341 de 2018, se actualiza el Mapa de Procesos en el que la gestión de riesgos deja de ser un proceso y se establece como un Programa que hace parte del Proceso de Direccionamiento y Planeación en cuanto a definición de la política y del Proceso Desarrollo del Sistema de Gestión en cuanto a su desarrollo e implementación, dando respuesta a criterios de acreditación en salud, que enmarca la gestión de riesgos como uno de sus ejes. Para el ciclo 2019 – 2020 se trabajó bajo estos parámetros.

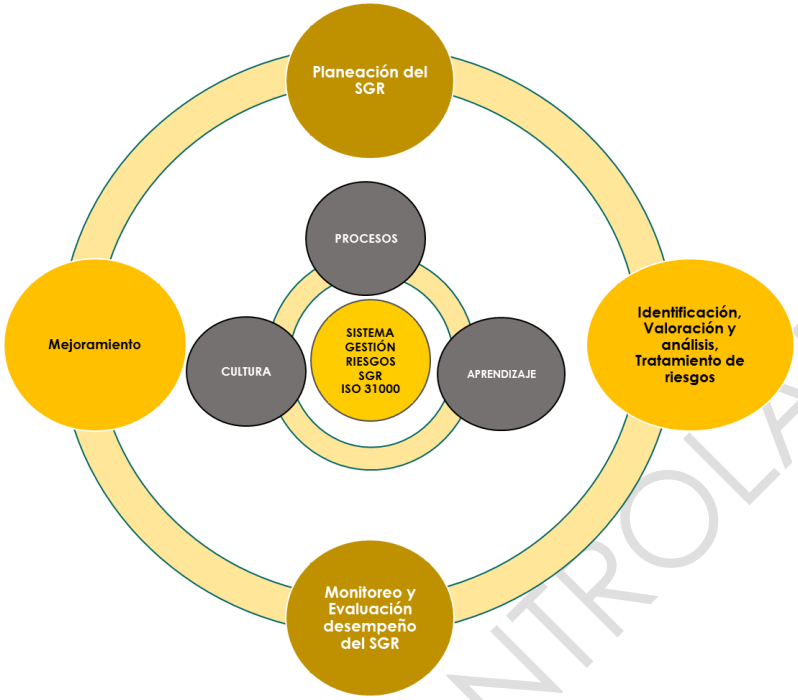


Fuente: Oficina Asesora de Planeación y Desarrollo Organizacional_2019

Para el nuevo ciclo de Gestión de Riesgos 2021 – 2022, se replantea este criterio y se retoma como sistema, en el marco del Sistema Integrado de Gestión de la empresa, el cual se desarrolla a través de los **Proyectos Gobierno Corporativo y Sistema de Gestión** del Plan de Desarrollo 2020 – 2025, como parte de la **Ruta Estratégica Gobierno Corporativo y Claridad Organizacional** de la **Estrategia Metrosalud Transparente, Clara, Inteligente e Innovadora.**

El Sistema de Gestión de Riesgos hace parte del Sistema Integrado de Gestión de la empresa y comprende como todos los sistemas que lo componen, tres ejes en los cuales se desarrolla: procesos, cultura y autorregulación – aprendizaje organizacional.

El esquema de la Gestión de Riesgos se muestra a continuación:



Fuente: Oficina Asesora de Planeación y Desarrollo Organizacional 2020

La ESE Metrosalud para la gestión de riesgos utiliza los conceptos contenidos en la NTC ISO 31000 Gestión del Riesgo, en la Guía para la Administración del Riesgos y el Diseño de Controles en Entidades Públicas vigente del DAFP y también los lineamientos para la supervisión basada en riesgos que ha emitido la Supersalud, buscando su articulación, dando claridad que a la fecha no se ha emitido lineamientos específicos para las Instituciones Prestadoras de Servicios de Salud IPS.

Igualmente integra a través de sus componentes los requerimientos normativos que se detallan en el marco normativo.

6. MARCO NORMATIVO

Tabla 1. Principal normatividad vigente relacionada con el Sistema de Gestión de Riesgos y sistemas asociados

Norma legal	Descripción
Decreto 1537 de 2001	Establece los elementos para el desarrollo y fortalecimiento del Control Interno en los organismos de la administración pública, entre los que se encuentra "Administración del Riesgo".

Norma legal	Descripción
Decreto 1499 de 2017	"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015", el cual adopta la versión actualizada del Modelo Integrado de Planeación y Gestión –MIPG, que incluye la gestión de riesgos
La Ley 1474 de 2011 Artículo 73, Decreto 1081 de 2015 titulo 4- Decreto Reglamentario 124 de 2016	Establecen los lineamientos para la elaboración del mapa de riesgos de corrupción en el marco del Plan Anticorrupción y de Atención al Ciudadano, alineado con directrices de la "Guía para la Gestión del riesgo de corrupción" de la Presidencia de la República.
Resolución 3100 de 2019 y Guía de Buenas Prácticas de Seguridad del Paciente del Ministerio de Salud y Protección Social	Manual de Estándares del Sistema Único de Habilitación, en el estándar 5 Proceso Prioritarios, obliga a las IPS la implementación de diez barreras de seguridad obligatorias, contenidas en la Guía de Buenas Prácticas de Seguridad del paciente del Ministerio de Salud y Protección Social y en los respectivos paquetes Instruccionales.
Circular 009 de 2016 de la Superintendencia Nacional de Salud	La que imparte instrucciones para la implementación del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo, como el fin de prevenir que la empresa sea utilizada para dar apariencia de legalidad a activos que proviene de actividades delictivas o que sean utilizadas para ocultar la procedencia de recursos que sean dirigidos a la realización de actividades terroristas.
Acuerdo 252 de 2014 que adopta el Manual de Contratación de la ESE Metrosalud,	El cual orienta la identificación de riesgos durante los procesos de contratación, con base en los lineamientos establecidos por Colombia Compra Eficiente.
Resolución 5095 de 2018 del Ministerio de Salud y Protección Social	Adopta el Manual de Acreditación en Salud Ambulatorio y Hospitalario, el cual comprende en los estándares de direccionamiento y en los estándares de gerencia el componente de un sistema de administración de riesgos articulado con el direccionamiento estratégico de la organización.
Decreto 1072 de 2015, Decreto Único Reglamentario del Sector Trabajo.	Establece el Sistema de Seguridad y Salud en el Trabajo, definiendo las directrices de obligatorio cumplimiento para su implementación en los sujetos obligados.
Ley 1523 de 2012	Obliga a las empresas a contar con un plan de prevención y atención de emergencias y desastres y su recuperación, acorde con la Política Nacional en la materia.

Norma legal	Descripción
Decreto 351 de 2014 Guía técnica colombiana GTC 24	Se reglamenta la gestión integral de los residuos generados en la atención en salud y otras actividades, como parte de la gestión ambiental y los riesgos asociados a esta.
Decreto 1078 de 2015	Respecto a la estrategia de Gobierno Digital -GD-, indica que las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información al interior de la entidad.
NTC ISO 14001 - 2015 – 2015	Sistemas de Gestión Ambiental. Requisitos con orientación para su uso

Norma Técnica	Descripción
NTC ISO - 31000	Gestión del riesgos: Directrices

7. EJES DEL SISTEMA DE GESTIÓN

El Sistema de Gestión de Riesgos encuentra su fundamento en el sistema integrado de gestión, y es a partir de allí donde se encuentra su articulación y verdadera sinergia. Los ejes que dan vida al sistema de gestión de riesgos son los siguientes:

- **Gestión de la cultura corporativa**, definida a través del sistema de significados y normas compartidos por los miembros de Metrosalud que determinan la manera cómo interactúan entre ellos y ellos con el entorno.
- **Gestión de procesos**, entendida como el análisis sistemático de los procesos organizacionales, de la cadena de valor y las relaciones que se generan a través de la interacción de sus elementos, con el fin de generar valor público asegurando el cumplimiento de los requisitos de calidad de sus productos y servicios de cara a sus clientes y grupos de interés, en el marco de los valores del servicio púbico. Incluye todas las etapas desde la planeación del proceso, pasando por su implementación, seguimiento a partir de indicadores hasta su evaluación y mejora a partir de evaluaciones o autoevaluaciones.
- **Aprendizaje**, entendido este como un proceso que permite mejorar el desempeño de la organización a través de la transformación de información generada por los procesos en nuevo conocimiento y capacidades para estos. A este se llega tomando como soporte todas las fuentes de instrumentos de auditoría o autoevaluación que disponga el sistema.

8. COMPONENTES Y ELEMENTOS DEL SISTEMA DE GESTIÓN

Para efectos del Sistema de Gestión de Riesgos, deben entenderse contenidos todos los elementos mencionados en el Marco Normativo y adicionalmente los riesgos por proceso.

Elementos Sistema de Gestión de Riesgos ESE Metrosalud

La gestión del riesgo en la ESE Metrosalud implica el desarrollo secuencial de varias actividades, a cargo de unos responsables establecidos en los lineamientos normativos externos e internos, que se detalla a continuación.

8.1 PLANEACIÓN DEL SISTEMA DE GESTIÓN

8.1.1 Roles y responsabilidades en la Gestión del Riesgo

La gestión del riesgo, alineado con la dimensión del MIPG de "Control Interno", se desarrolla a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en los servidores de la entidad como sigue:

LINEA ESTRATÉGICA
Define el marco general para la gestión de riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el Comité Institucional de Coordinación de Control Interno

1° LÍNEA DE DEFENSA	2° LÍNEA DE DEFENSA	3° LÍNEA DE DEFENSA
Desarrolla e implementa proceso de control y gestión de riesgos a través de su identificación, análisis, valoración y monitoreo y acciones de mejora	Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	Proporciona información sobre la efectividad del S.C.I. a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.
⬇	⬇	⬇
A cargo de los gerentes públicos y líderes de procesos, programas y proyectos de la entidad. Rol Principal: diseñar, implementar y monitorear los controles, además 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	A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefe de Planeación y Desarrollo Organizacional, Supervisores de contratos y/o proyectos, Comité de Adjudicaciones y Recomendaciones, Comité de Seguridad el Paciente, Líderes de Subsistemas de Gestión. Rol principal: monitorear la gestión de riesgo y control	A cargo de la Oficina de Control Interno, auditoría interna o quién haga sus veces. Rol Principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I El alcance de este aseguramiento, a través de la auditoría interna

metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro. Comité Institucional de Evaluación y Desempeño, Comité de Gerencia y Responsables de los procesos.	ejecutada por la primera línea de defensa. Complementando su trabajo	cubre todos los componentes del S.C.I

En la ESE Metrosalud, se establecen las siguientes responsabilidades acorde con dicho esquema:

La Junta Directiva debe conocer claramente la capacidad de la Organización para asumir riesgos en relación con los objetivos y metas del negocio. La Gestión del Riesgo desde el alto nivel crea ventaja competitiva y genera valor	
Junta Directiva	Proponer mecanismos para fomentar la cultura de seguridad y gestión del riesgo en la empresa, que lleven al desarrollo de hábitos de control de riesgos en los procesos de la organización.
	Avalar la Política Lavado de Activos y Financiación del Terrorismo y los lineamientos generales que lo definen.
	Designar el Oficial de Cumplimiento y su respectivo suplente, en lo relacionado con el SARLAFT (Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo).
	Hacer seguimiento a la implementación del SARLAFT y pronunciarse sobre los informes del SARLAFT presentados por el Oficial de Cumplimiento y el Revisor Fiscal

Comité de Coordinación de Control Interno Línea estratégica
• Participar en el establecimiento de la Política y el Sistema de Gestión de Riesgos de la
• Orientar y monitorear la implementación de las estrategias del Sistema de Gestión del
• Realizar análisis de eventos y riesgos críticos.
• Monitorear los indicadores del Sistema de Gestión de Riesgos.
• Proponer a la Gerencia y al Comité de Evaluación y Desempeño la implementación de estrategias que fortalezcan la gestión de riesgos en la organización.

Comité de Gerencia – Responsables de los procesos 1° línea de defensa.
• Establecer la Política y el Sistema de Gestión de Riesgos de la Empresa.
• Definir el contexto estratégico, contexto interno y los criterios para la gestión de riesgos.

Comité de Gerencia – Responsables de los procesos 1° línea de defensa.
• Desplegar e implementar mecanismos para fomentar la cultura de gestión del riesgo en la empresa, que lleven al desarrollo de hábitos de control de riesgos en los procesos de la organización
• Fomentar la autocapacitación y la capacitación de los equipos en la gestión de
• Cumplir y monitorear la efectividad de los controles y acciones de tratamiento de riesgos definidas para cada uno de los procesos institucionales que tienen a su cargo.
• Definir las acciones correctivas y preventivas para mitigar los riesgos identificados de los procesos.
• Disponer los recursos físicos, económicos, tecnológicos y de talento humano necesarios para el establecimiento y desarrollo del Sistema de Gestión de Riesgos

Comité Institucional de Evaluación y Desempeño - 1° línea de defensa
• Supervisar y analizar periódicamente la gestión de riesgos y los resultados obtenidos, proponiendo acciones correctivas necesarias.
• Estimular la cultura de gestión y prevención de riesgos, involucrando a los Directivos y sus equipos de trabajo y Responsables de Procesos, en la identificación, análisis, tratamiento y monitoreo de los riesgos relacionados a los procesos a su cargo.

Directivos - Responsables de los procesos - Equipos de trabajo 1° línea de defensa
• Identificar, analizar y valorar los riesgos del proceso, aplicando la metodología e instrumentos definidos por la norma y la institución.
• Definir e implementar controles y/o barreras de seguridad de los procedimientos acorde con los lineamientos institucionales vigentes de diseño e implementación
• Elaborar el Plan de Tratamiento de Riesgos del proceso a su cargo.
• Ejecutar las acciones de tratamiento de riesgos a su cargo
• Monitorear la efectividad de los controles definidos en el mapa de riesgos y en su
• Monitorear los indicadores del Sistema de Gestión de Riesgos del proceso a su cargo.
• Desplegar e implementar los mecanismos establecidos para fomentar la cultura de seguridad y gestión del riesgo en la empresa, que lleven al desarrollo de hábitos de control de riesgos en los procesos de la organización.
• Definir las acciones correctivas y preventivas para mitigar los riesgos identificados de los procesos.

Servidor Público 1° línea de defensa
• Identificar los riesgos en el desempeño de su trabajo y para el usuario en el día a día.
• Proponer controles para evitar la materialización del riesgo y/o mitigar sus
• Implementar los controles en las actividades y tareas que ejecuta, como principio de autocontrol.
• Reportar al Oficial de Cumplimiento cualquier señal de alerta, operación inusual o sospechosa en lo relacionado con el SARLAFT (Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo).
• Participar en las capacitaciones que brinde la empresa en temas de gestión de riesgos

Comité de Seguridad del Paciente 2° línea de defensa
• Orientar y monitorear la implementación de las estrategias de seguridad del paciente
• Monitorear los indicadores del Programa de Seguridad del Paciente y la implementación de las prácticas seguras
• Proponer a la Gerencia y al Comité de Gerencia la implementación de estrategias que fortalezcan la gestión de Seguridad del Paciente en la organización.
• Gestionar los eventos adversos a través de los referentes de seguridad del paciente de

2° línea de defensa: Oficina Asesora Planeación y Desarrollo Organizacional – Líderes de otros sistemas de gestión – Comité de Recomendaciones y Adjudicaciones – Supervisores de contratos y proyectos
• Asesoría en la implementación del sistema de gestión a cargo
• Monitorear la gestión de riesgo definida por la primera línea de defensa
• Monitorear la efectividad de los controles definidos en el mapa de riesgos y del proceso y/o sistema de gestión a cargo

Revisor fiscal
• Rendir por lo menos anualmente informe a la Junta Directiva sobre el cumplimiento o incumplimiento de las disposiciones contenidas en el SARLAFT (Sistema de Administración de Riesgos de Lavado de Activos Y Financiación del Terrorismo).
• Informar al Oficial de Cumplimiento las inconsistencias y falencias con respecto a la implementación del SARLAFT.

- Rendir informes sobre el cumplimiento de la normativa vigente sobre el SARLAFT, que la Superintendencia Nacional de Salud le solicite.

8.1.2 Diseño del proceso

- Establecer el contexto.
- Identificar los riesgos.
- Valorar y analizar los riesgos
- Tratar los riesgos.
- Monitorear y revisar.
- Comunicar.

8.1.3 Establecer el contexto

Establecer el contexto externo

Define la relación de la ESE Metrosalud con su entorno, determina las características o aspectos esenciales del medio en el cual opera la entidad, identificando fortalezas, debilidades, oportunidades y amenazas, siguiendo la metodología definida en la entidad para la construcción del Plan de Desarrollo. Se tienen en cuenta aspectos políticos, económicos / financieros, sociales / culturales, tecnológicos, ambientales y legales / reglamentarios.

El contexto externo se actualiza de acuerdo con los resultados de la evaluación del Plan de Desarrollo y de la Estrategia Organizacional cada que éste se formule y en aquellos casos extraordinarios que se requiera, acorde con metodología que tiene vigente la empresa para este fin.

Esta actividad no se realiza de manera independiente para el Sistema de Gestión de Riesgos, se acoge a la actualización que se lleva a cabo en el marco de formulación del Plan de Desarrollo vigente en la empresa y las actualizaciones que se lleven a cabo.

Establecer el contexto interno

Establecer el contexto interno, implica conocer y comprender la organización, sus metas, objetivos y estrategias, determina las características o aspectos esenciales del ambiente en el que la organización busca alcanzar sus objetivos y que influye en la forma como la organización gestiona sus riesgos. Incluye factores como estructura organizacional, funciones/responsabilidades, políticas, objetivos y estrategias implementadas, recursos (económicos, personas, procesos, sistemas, tecnología e información), conocimientos con que se cuenta, relaciones con las partes involucradas y cultura organizacional.

El no lograr los objetivos de la organización, sistema, modelo, plan, proceso o proyecto, representa un conjunto de riesgos que deben tratarse.

De manera similar al contexto externo, el contexto interno se actualiza de acuerdo con los resultados de la evaluación del Plan de Desarrollo y de la Estrategia Organizacional, conforme a la periodicidad definida para su formulación en la empresa y en aquellos casos extraordinarios que se requiera, acorde con metodología que tiene vigente la empresa para este fin.

Tanto el contexto externo como interno realizado durante el proceso de formulación y actualización de Plan de Desarrollo serán el referente para la gestión de los riesgos para los Directivos y sus equipos de trabajo y demás responsables de procesos, sistemas , modelos, planes, programas y proyectos.

Establecer el contexto de la gestión del riesgo

Esta etapa incluye la revisión y determinación de las características o aspectos esenciales de la gestión del riesgo en la empresa, teniendo en cuenta factores como: objetivo y alcance, interrelación con los procesos y procedimientos.

Como herramienta básica para el análisis, se utiliza la caracterización de los procesos vigentes en la empresa y sus procedimientos.

Se tienen en cuenta además, las metas y objetivos de la gestión del riesgo, roles y responsabilidades, alcance y profundidad de las actividades en gestión del riesgo, metodologías de valoración de riesgos y formas de evaluar el desempeño y eficacia en la gestión del riesgo, temáticas descritas a lo largo de este documento.

Por parte del Equipo Directivo como responsables de los procesos y del Comité de Coordinación de Control Interno, se establece la clasificación y factores de riesgo aplicables a la empresa y su relación, se determinan así mismo los criterios de calificación del riesgo y conceptos asociados a cada valor, mediante las tablas de valoración de riesgo, los cuales se describen en las etapas de identificación y valoración de los riesgos. Estos deben ser revisados y ajustados cada dos años con los ciclos de gestión de riesgos o en el momento que se requiera si las condiciones normativas u organizacionales así lo exigen.

La empresa dispone de un aplicativo para el manejo integral de su sistema de gestión organizacional, el cual incluye un módulo de riesgos, mediante el cual se elabora el mapa de riesgos institucional y el plan de tratamiento de riesgos que de este se derive. Este módulo se parametriza en relación con el mapa de procesos de la empresa, de forma que los riesgos y las actividades de tratamiento correspondientes, se gestionan a través de cada proceso. Para el caso de riesgos de elementos organizacionales que no se constituyen un proceso en si mismo, se analizan en el proceso al que le corresponde su gestión.

Apetito y tolerancia del riesgo

El apetito de riesgo, la tolerancia y la capacidad de riesgo son términos utilizados para establecer los niveles de riesgo aceptables en una organización y sus valores deben ser determinados con la participación y aprobación de la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno.

Es importante definir inicialmente el **nivel de riesgo**, que 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.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad bajo los requisitos del marco legal aplicable puede soportar y a partir del cual la alta dirección consideran que no sería posible el logro de los objetivos de la entidad y corresponden a los riesgos residuales calificados como nivel extremo.

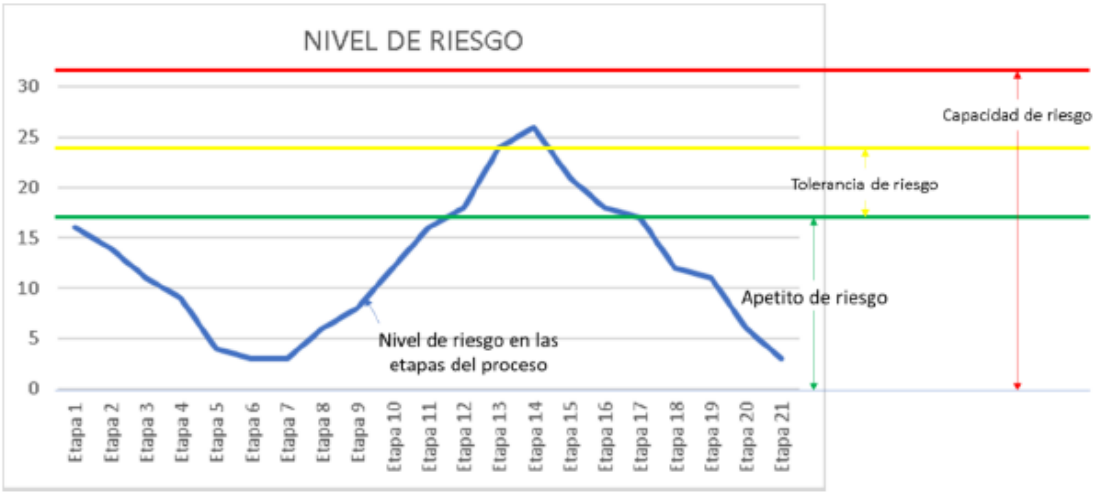
Apetito de riesgo: Es el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del Modelo Integrado de Planeación y Gestión en la entidad, es decir, el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar, en general corresponde a los riesgos residuales que quedan calificados en nivel bajo.

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.
Es un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo, nunca puede ser superior al valor de esta última y corresponde a los riesgos residuales calificados como nivel medio y alto.

La determinación de la tolerancia de riesgo, es optativa y está orientada a determinar el tipo de acciones para abordar los riesgos, que se desprendan a partir del análisis de riesgos y que deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo

Gráficamente los anteriores conceptos se relacionan así:



Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

Fuente: Guía de administración de riesgos y diseño de controles en entidades publicas 2020

Los niveles de riesgo en el mapa de calor en relación con el apetito, tolerancia y capacidad y acciones a realizar se muestran en la siguiente tabla:

Nivel del riesgo	NIVEL DE ACEPTABILIDAD	ACCIÓN
Extremo	**Inaceptable.**	Requiere acciones de intervención de alta prioridad
Alto	**Grave.**	Requiere acciones de intervención a corto plazo
Moderado	**Tolerable.**	Requiere acciones de intervención a mediano plazo
Bajo	**Aceptable.**	No requiere acciones diferentes a las ya implementadas, o son a más largo plazo

Establecer el contexto del riesgo implica además, la validación y estandarización de los equipos de trabajo con los responsables de los procesos en la metodología de gestión de riesgos institucional, ya que son ellos los responsables de su aplicación, desde la identificación de los riesgos y el seguimiento a los resultados, así como la definición de controles y/o barreras de seguridad y el seguimiento a su efectividad desde el autocontrol.

En esta etapa se define el elemento a evaluar: objetivo institucional, sistema, modelo, plan, programa, proyecto o proceso, con su objetivo, revisando la articulación con los objetivos institucionales

Riesgos de Corrupción

Para los riesgos de corrupción deben tenerse en cuenta los lineamientos de la "Guía de Riesgos de Corrupción" de la Presidencia de la República, la cual se encuentra alineada con la Guía para la Administración del Riesgo del DAFP Octubre 2020, por tanto se desarrollan las etapas en una sola matriz de riesgos por proceso, que los incluye.

Según la "Guía de Riesgos de Corrupción" de la Presidencia de la República, se define riesgo de corrupción como la "Posibilidad de que por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado".

Para la identificación y valoración de los riesgos de corrupción se utiliza la matriz de riesgos por proceso consolidada, que los incluye. Es necesario que en la descripción del riesgo concurran los componentes de su definición: acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

Si al describir un riesgo, aplican todos los componentes enunciados anteriormente, se constituye un riesgo de corrupción, por lo que deberá ser tenido en cuenta para su posterior análisis.

En la tabla siguiente se presentan los riesgos de corrupción establecidos por el Equipo Directivo con la descripción de cada uno en cumplimiento de los componentes mencionados anteriormente.

MATRIZ DEFINICIÓN RIESGOS DE CORRUPCIÓN 2019					
Descripción del riesgo	Acción y Omisión	Uso del poder	Desviar la gestión de lo público	Beneficio particular	Proceso Impactado
1. Tráfico de influencias, (amiguismo, persona influyente, clientelismo)	Utilizar indebidamente influencias derivadas del ejercicio del cargo o de la función	Mediante el amiguismo, clientelismo o persona influyente	Impidiendo o menguando el acceso a la información y/o la capacidad de oferta a la institución	Favoreciendo con información, recursos o bienes de la administración pública a un servidor específicamente o a una organización, en un asunto que éste se encuentre conociendo o	G bienes y servicios (contratación) G talento humano G financiera G. Salud Pública y Territorial G. Venta de Servicios G. Coactiva

MATRIZ DEFINICIÓN RIESGOS DE CORRUPCIÓN 2019					
Descripción del riesgo	Acción y Omisión	Uso del poder	Desviar la gestión de lo público	Beneficio particular	Proceso Impactado
				haya de conocer	
2. Extralimitación de funciones y/o concentración de autoridad o exceso de poder	Desconocimiento de límites y responsabilidades de cargos, y áreas y de las actividades definidas en el Manual de Funciones	Abusando de las funciones y responsabilidades asignadas y/o concentrando las decisiones y/o el uso de los recursos	Cometiendo acto arbitrario e injusto, generando desconfianza, deterioro del clima laboral, retraso o reprocesos en la operación	Facilitando el acoso laboral, la entrega inoportuna e incompleta de la información solicitada, acomodándolos a intereses particulares	Direccionamiento Estratégico G Sistemas de información G bienes y servicios (contratación) G talento humano G. Coactiva G. Salud Pública y Territorial
3. Soborno (cohecho - recibir dádivas)	Realizar, adelantar, omitir o retardar actos propios de su cargo	Desarrollando su trabajo con negligencia en los procedimientos y trámites requeridos	Actuando en consonancia, para recibir dadivas, dineros o beneficios	Buscando el favorecimiento indebido de un servidor, un ciudadano o una empresa	G bienes y servicios (contratación) G talento humano G. Coactiva
4. Cobro por realización del trámite (Concusión)	Inducir a dar o prometer o solicitar al ciudadano o empresa, dinero u otra utilidad por la realización del trámite o servicios	Exigir dinero y dádivas para el desarrollo de un trámite que por ley no tiene ningún costo	Conductas violatorias de la ley por parte del servidor público	Buscando el favorecimiento indebido de un servidor, un ciudadano o una empresa	G bienes y servicios (contratación) G talento humano G. Coactiva

MATRIZ DEFINICIÓN RIESGOS DE CORRUPCIÓN 2019					
Descripción del riesgo	Acción y Omisión	Uso del poder	Desviar la gestión de lo público	Beneficio particular	Proceso Impactado
5. Ocultación o adulteración del sistema de información y/o filtración de información confidencial	Ocultación, adulteración o acceso no autorizado a las bases de datos e información tanto no confidencial como confidencial	Manipulando las fuentes de información, los informes o registros del sistema de información y/o filtrando información confidencial	Poniendo en tela de juicio la veracidad y calidad de los datos y/o facilitando el acceso a información confidencial a terceros no autorizados	Presentando información parcializada o fraudulenta y/o entregando información confidencial a terceros no autorizados, para el interés propio de una institución, servidor o ciudadano.	G Sistemas de información G bienes y servicios (contratación) G talento humano G Jurídica G procesos disciplinarios G Jurídica G. Coactiva
6. Manipulación del proceso definido en la normatividad externa e interna, a favor de un tercero, en relación con procesos disciplinarios, contratación de bienes y servicios, ingreso de persona y financiero, entre otros.	Incumplimiento y separación de lineamientos normativos externo e internos en relación con procesos disciplinarios, contratación de bienes y servicios, ingreso de personal y financiero entre otros.	Manipulación y/o modificación de los lineamientos institucionales definidos	Conductas violatorias de lineamientos institucionales, generando desconfianza, deterioro del clima laboral, retrasos o reprocesos	Facilitando beneficios y ventajas para un servidor, un tercero o institución	G Sistemas de información G bienes y servicios (contratación) G talento humano G Jurídica G. Coactiva G. Salud Pública y Territorial

MATRIZ DEFINICIÓN RIESGOS DE CORRUPCIÓN 2019					
Descripción del riesgo	Acción y Omisión	Uso del poder	Desviar la gestión de lo público	Beneficio particular	Proceso Impactado
7. Peculado por apropiación, omisión o aplicación oficial diferente de bienes del Estado o extravío, pérdida o daño de estos	Apropiación, omisión o aplicación oficial diferente de bienes del Estado	Negligencia, extravío, pérdida o daño en la administración, tenencia o custodia de bienes del Estado, que se le haya confiado por razón o con ocasión de sus funciones	Conductas violatorias de la ley por parte del servidor público	Buscando el favorecimiento indebido de un servidor, un ciudadano o una empresa	G financiero G bienes y servicios Atención farmacéutico G. Salud Pública y Territorial

Fuente: "Guía de Riesgos de Corrupción" Presidencia de la República y Plan Anticorrupción y Atención al ciudadano ESE Metrosalud 2021.

Riesgos de Lavado de Activos y Financiación del Terrorismo LA/FT:

Para los riesgos de Lavado de Activos y Financiación del Terrorismo se tienen en cuenta los lineamientos de la Circular 009 de 2016 de la Superintendencia Nacional de Salud, y el Manual SARLAFT vigente en la empresa, y éste se integra con el mapa de riesgos institucional. Los controles se encuentran definidos en el Manual e instructivos asociados al Proceso Desarrollo del Sistema de Gestión.

8.2 IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN

8.2.1 Identificar los riesgos

Para el desarrollo de esta y las siguientes etapas, hasta el Plan de Tratamiento de riesgos, se utilizará como instrumento la Matriz de Riesgos por proceso vigente en la empresa en el aplicativo SGI Almera

En este paso se identifican los riesgos del elemento organizacional analizado, incluidos aquellos identificados en las auditorías internas que realiza la Oficina de Control Interno y Evaluación, lo reportado a Mesa de Ayuda riesgos o las que sean identificadas por otras fuentes y que sean de importancia para la organización.

El objetivo de esta etapa es identificar los riesgos reales o potenciales, que pudieran retrasar el logro de los objetivos de los procesos, de los objetivos corporativos y de los demás elementos organizacionales asociados a cada proceso.

En la etapa de identificación de riesgos es importante incluir las personas que conocen suficientemente el proceso objeto de análisis como sus responsables con sus equipos de trabajo, pero también se considera importante tener en cuenta a aquellas personas, que mantienen relación directa con el proceso a evaluar, ya sea porque son clientes o proveedores del mismo en la cadena de valor. De esta manera se puede hacer un análisis integral de la gestión del riesgo del proceso.

Análisis de objetivos estratégicos y de los procesos: Todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

- Se deben analizar los objetivos estratégicos y los posibles riesgos que afecten su cumplimiento y que puedan ocasionar su éxito o su fracaso, que estén alineados con el Propósito Superior, la Misión y Visión, así también su desdoble hacia los objetivos de los procesos.
- Se analizan los objetivos de proceso que estén alineados con el Propósito Superior, la Misión y Visión y que contribuyan con los objetivos estratégicos.

Estos deben incluir el que, cómo, cuándo, para y porque, para poder aplicar la metodología de gestión de riesgos.

Identificación de puntos de riesgo: Son aquellas actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Se debe tener en cuenta la eficiencia en el uso de los recursos durante la ejecución y la eficacia en el cumplimiento de los objetivos para el logro de los resultados, teniendo en cuenta las entradas y salidas del proceso

Identificación de áreas de impacto: Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional. Y sobre estos se realiza la valoración del impacto en la matriz de riesgos.

Identificación de áreas de factores de riesgo: Son las fuentes generadoras de riesgos.

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización en la ejecución de los procesos	Falta de procesos y/o procedimientos
		Deficiencias en la adherencia a los procesos y procedimientos
		Fallas en el mejoramiento de los procesos.
		Errores en la información generada de los procesos
		Falta de capacitación
		Deficiencias en temas relacionados con el personal y la administración de personal
		Retrasos o errores en los procesos de contratación
		Deficiencias en la supervisión de contratos
Talento Humano	Incluye Sistema de Seguridad y Salud en el Trabajo SG-SST. Se tiene en cuenta además posible dolo e intención frente a los riesgos de corrupción definidos en la organización	Deficiencias en la implementación del Sistema de Seguridad y Salud en el Trabajo SG-SST
		Hurto activos
		Posibles comportamientos no éticos o no adecuados, de forma deliberada de los empleados
		Fraude interno asociado a riesgos de corrupción
Tecnología biomédica e insumos generales y hospitalarios	Eventos relacionados con la tecnológica biomédica y con los insumos generales y hospitalarios.	Insuficiencia de equipos biomédicos y sus especificaciones técnicas
		Desabastecimiento de insumos generales y hospitalarios.
		Deficiencias en el mantenimiento preventivo y correctivo de equipos biomédicos
Infraestructura, equipos industriales y tecnología informática	Eventos relacionados con la infraestructura física de la entidad por causas internas, equipos industriales y hardware y software requeridos para la operación	Incendios
		Inundaciones
		Daños a activos fijos e instalaciones
		Caída de aplicaciones
		Caída de redes
		Errores en programas
		Deficiencia de tecnología informática

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Financiero	Eventos relacionados con la generación de ingresos y cobro a entidades contratantes.	Deficiencias en los procesos de facturación
		Condiciones operativas y financieras desfavorables en la contratación de venta de servicios de salud
		Ventas insuficientes para lograr el equilibrio financiero
Evento Externo	Situaciones externas que afectan la entidad	Atentados, vandalismo, orden público
		Suplantación de identidad
		Asaltos a las sedes
		Situación del sector salud.
		Fraude Externo
		Influencias políticas
		Entidades aseguradoras sin capacidad financiera

Estos factores de riesgo están sujetos a modificación si la dinámica de la empresa así lo requiere, incluyendo factores y/o descripciones adicionales.

Descripción del riesgo

Para la identificación de riesgos se utilizan herramientas como, lluvia de ideas, listas de chequeo o juicio de expertos, a través de un proceso estructurado, ya que un riesgo potencial no detectado en esta etapa, será excluido del análisis posterior.

Esta identificación se hace con base en los **puntos de riesgo** identificados en los procesos y procedimientos y en las **áreas de factores de riesgos**, definidas en el presente documento para la organización.

Se genera con estos insumos, una relación de riesgos reales o potenciales para cada objetivo estratégico y cada proceso, que pueden impedir el cumplimiento de los objetivos del elemento sobre el que se hace el análisis.

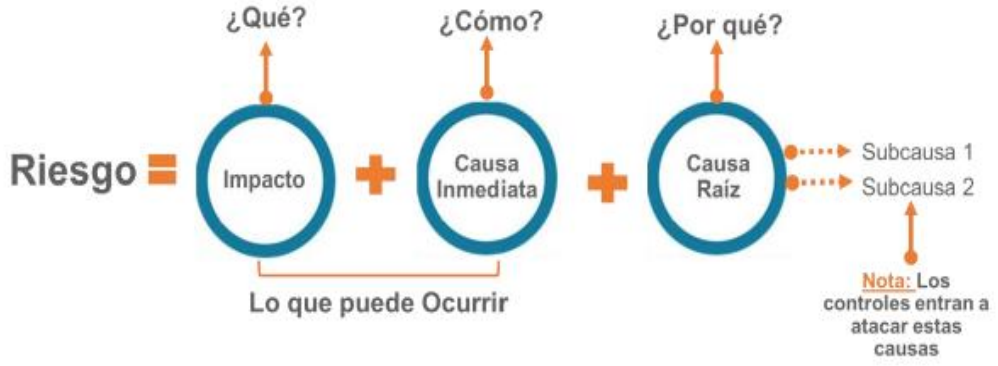
Es importante establecer los eventos que impiden dicho cumplimiento, con enfoque en el usuario, en su seguridad y en el proceso de atención. Igualmente, considerar los eventos de corrupción y de lavado de activos y financiación del terrorismo asociados al elemento analizado (sistema, modelo, plan, programa, proyecto o proceso).

En cuanto a los riesgos de corrupción, estos son definidos por el Equipo Directivo de la empresa acorde con criterios dados por la Secretaría de Transparencia de la Presidencia de la República, como se explicó anteriormente.

Para la redacción de los riesgos se propone la siguiente estructura, con el fin de lograr mayor objetividad, manifestando las causas mediatas e inmediatas, que son necesarias para la definición de los controles.

Se propone una estructura que facilita su redacción y claridad, que inicia con la frase POSIBILIDAD DE y se tienen cuenta los siguientes aspectos:

- Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.



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

Fuente: Guía de administración de riesgos y diseño de controles en entidades públicas 2020

Ejemplo:

Qué	Cómo	Por qué
Posibilidad de Afectación Económica	Por multa o sanción del ente regulador	debido a adquisición de bienes y servicios fuera de los Requerimientos normativos

Premisas para una adecuada redacción del riesgo

- No describir como riesgos omisiones ni desviaciones del control.
  Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

- No describir causas como riesgos
  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- No describir riesgos como la negación de un control.
  Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

- No existen riesgos transversales, lo que pueden existir son causas transversales. Puede ser un riesgo asociado a varios procesos, y en cada uno los controles son diferentes.
  Ejemplo: pérdida de expedientes.

Clasificación del riesgo:

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Clasificación	Descripción
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad, en las cuales está involucrado por lo menos 1

Clasificación	Descripción
	participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales

Esta clasificación de riegos se asocia con los factores de riesgos de la siguiente forma:

Clasificación del riesgo	Relación	Factores de riesgo
Ejecución y administración de procesos	→	Procesos
Fraude externo	→	Evento Externo
Fraude interno	→	Talento Humano
Fallas tecnológicas	→	Tecnología Evento Externo
Relaciones laborales	→	Procesos Talento Humano Tecnología Otros
Usuarios, productos y prácticas	→	Procesos Talento Humano Tecnología Otros

Daños a activos fijos/ eventos externos	→	Infraestructura e Insumos Evento Externo

Tipologías del riesgo

Una vez identificado y clasificado un riesgo, éste puede ser además catalogado en una de las siguientes tipologías:

- Estratégico y Gerenciales: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública, y/o alta dirección y por tanto impacta toda la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y contextualización de la entidad.

- Operativo: desviaciones en los objetivos misionales de sus procesos como consecuencia de deficiencias, inadecuaciones o fallas en los procesos, en el recurso humano, en los sistemas biomédicos, en la infraestructura, ya sea por causa interna o por la ocurrencia de acontecimientos externos, entre otros.

  Estos incluyen:

  Gestión de riesgo en salud es la probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa o la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse. El evento, es la ocurrencia de la enfermedad, traumatismos a su evolución negativa, desfavorable a complicaciones de la misma; y las causas, son los diferentes factores asociados a los eventos.

- Reputacional o de Imagen: posibilidad de una acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de una entidad, tales como el impacto de la publicidad negativa sobre las prácticas comerciales, conducta o situación financiera de la entidad. Tal publicidad negativa, ya sea verdadera o no, puede mermar la confianza pública en la entidad, dar lugar a litigios costosos, o dar lugar a una disminución de su base de usuarios, clientes, negocios o los ingresos. De acuerdo con la capacidad de prevención mitigación pueden ser desagregados, en situacional o previsto.
  - Riesgo reputacional situacional: inmediato derivado de una acción imposible de anticipar.
  - Riesgo reputacional previsto: derivado de eventos a los cuales la organización puede anticiparse con una gestión adecuada de los riesgos en salud, financieros, y operativos, así como mediante estrategias de comunicación.

- Financiero: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, facturación, etc. Estos incluyen:
  - ✓ Liquidez: posibilidad que una entidad no cuente con recursos líquidos para cumplir con sus obligaciones de pago tanto en el corto (riesgo inminente) como en el mediano y largo plazo (riesgo latente).
  - ✓ Crédito: pérdidas como consecuencia del incumplimiento de las obligaciones por parte de sus deudores en los términos acordados, como, por ejemplo, monto, plazo y demás condiciones
  - ✓ Mercado de capitales: pérdidas derivadas de un incremento no esperado, de sus obligaciones con acreedores tanto internos como externos, o la pérdida en el valor de sus activos.

- Cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

- Riesgos de corrupción: posibilidad que una entidad presente desviaciones en los objetivos misionales de sus procesos como consecuencia de fraude y corrupción; posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. Las variables a tener en cuenta son:

  Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

  Integridad: propiedad de exactitud y completitud.

  Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

  Aquí se incluyen los riesgos tecnológicos, entendidos como la posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad, como virus, el vandalismo puro y de ocio en las redes informáticas, fraudes, intrusiones por hackers, el colapso de las telecomunicaciones que pueden generar el daño de la información o la interrupción del servicio.

- Riesgo de fallas de mercado: posibilidad que la estructura del mercado de salud genere pérdidas en el bienestar y beneficios de la entidad, como mercado monopólico u oligopólico y prácticas de competencia desleal.

- Medio Ambiente: Se refiere a los efectos resultantes de las actividades de la entidad, que generan un impacto negativo en el ambiente.

- Riesgos de Lavado de Activos y Financiación del Terrorismo LA/FT: posibilidad que, en la realización de las operaciones la entidad pueda ser utilizadas por organizaciones criminales como instrumento para ocultar, manejar, invertir o aprovechar dineros, recursos y cualquier otro tipo de bienes provenientes de actividades delictivas a destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas, a las transacciones y fondos de recursos vinculados con las mismas.
  De este riesgo se derivan otros ya descritos en esta categorización del riesgo como son riesgo legal, riesgo operativo, riesgo reputacional. Adicionalmente se incluye aquí el siguiente:
  - ✓ Riesgo de contagio: Pérdida que una empresa puede sufrir, directa o indirectamente, por una acción o experiencia de un relacionado o asociado. El relacionado o asociado incluye personas naturales o jurídicas que tienen posibilidad de ejercer influencia sobre la empresa.

8.2.2 Valorar los riesgos

Esta etapa consiste en realizar la valoración de cada riesgo la cual consiste en establecer la posibilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo inherente o absoluto).

Se desarrolla a través de los siguientes elementos:

Análisis de Riesgos	Evaluación de riesgos
Establecer la posibilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial **(Riesgo inherente o absoluto).**	Confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final **(Riesgo residual)**

8.2.2.1 **Determinar la probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo.

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.**

Así se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, dando mayor objetividad a la valoración.

Durante la actualización del mapa de riesgos con cada proceso, se establecerá con los equipos de trabajo las frecuencias para las actividades principales asociadas a los riesgos, como referente para la valoración de la probabilidad:

Criterios para definir el nivel de probabilidad

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

Guía de Administración de riesgos y diseño de controles para entidades públicas 2020

8.2.2.2 **Determinar el impacto:** se definen los impactos económicos y reputacionales como las variables principales.

Temas como las afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional.

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.

	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/o de proveedores.
Mayor 80%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Moderado 60%	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.

Guía de Administración de riesgos y diseño de controles para entidades públicas 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.
El análisis y la valoración de riesgos, se realiza cada dos años, acorde con el ciclo general de gestión de riesgos, con monitoreo y actualizaciones periódicas si se requieren por riesgos emergentes o materialización de riesgos, acorde con la dinámica organizacional y resultados de los seguimientos. En este caso el líder del proceso solicita el acompañamiento a la Oficina Asesora de Planeación y Desarrollo Organizacional para la respectiva actualización del mapa de riesgo del proceso.

8.2.2.3 Evaluación del Riesgo.

Se realiza a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias.

Análisis Preliminar <u>Riesgo inherente</u>

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Probabilidad						
	Muy alta 100%	Alto	Alto	Alto	Alto	Extremo
	Alta 80%	Moderado	Moderado	Alto	Alto	Extremo
	Media 60%	Moderado	Moderado	Moderado	Alto	Extremo
	Baja 40%	Bajo	Moderado	Moderado	Alto	Extremo
	Muy baja%	Bajo	Bajo	Moderado	Alto	Extremo
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
		Impacto				

Extremo
Alto
Moderado
Bajo

Analizar el riesgo implica la combinación de la estimación de Probabilidad (Frecuencia: número de veces que se pasa por el punto de riesgo en el periodo de un (1) año) e Impacto.

Para cada riesgo real o potencial, determine el impacto, si este ocurriera, y su probabilidad de ocurrencia, teniendo en cuenta los criterios en las tablas de valoración, descritas previamente.

La valoración final de la Probabilidad e impacto, así como la calificación de controles (se explica más adelante), se determina por consenso entre los miembros del equipo.

De no llegarse a consenso, la calificación será la moda entre los valores obtenidos. En caso de dos o más modas, la calificación final será la moda de mayor valor o nivel.

Los **riesgos de corrupción**, en cuanto a la severidad o impacto, **solo se califican en niveles moderado, mayor, o catastrófico**, bajo la premisa de que su presentación es siempre inaceptable, con consecuencias graves para la organización. **Nunca serán calificados como insignificante o menor.**

Para la valoración del impacto de los riesgos de corrupción, se tendrán en cuenta las preguntas relacionadas en la "Guía de Riesgos de Corrupción" de la Presidencia de la República, presentada anteriormente en el ítem de contexto de gestión de riesgos.

Con esta valoración del riesgo, antes de establecer y valorar los controles, se obtiene el **Riesgo Inherente o absoluto,** que es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

8.2.2.4 Determinación y Valoración de controles.

Como medio para alcanzar el logro de los objetivos, las actividades de control se orientan a prevenir, detectar y/o corregir la materialización de los riesgos, lo cual corresponde a la primera línea de defensa.

Conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

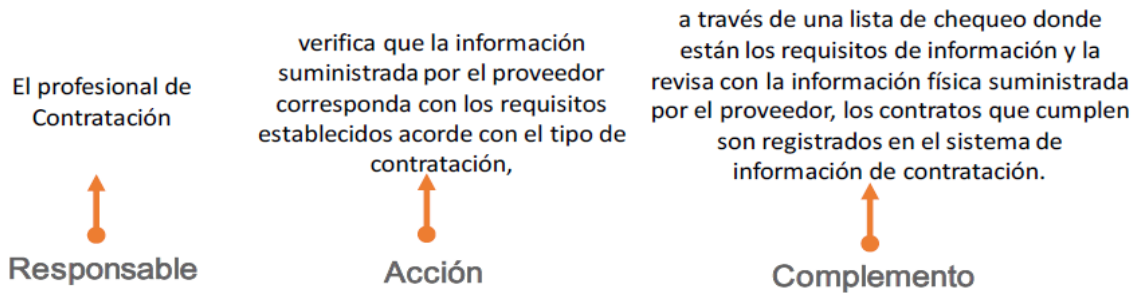
- La identificación de controles se debe realizar a cada riesgo y orientado a las causas raíz, a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer (Equipos por proceso). En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo, como primera línea de defensa.

Estructura para la descripción del control

La siguiente estructura facilitará entender su tipología y otros atributos para su valoración:

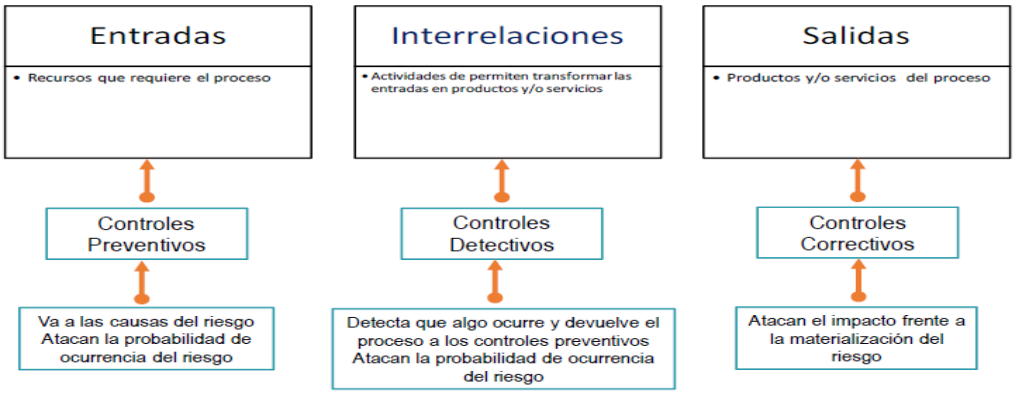
- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo:



Tipología de controles y los procesos

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la siguiente figura se consideran 3 fases globales del ciclo de un proceso así:



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

Fuente: Guía de administración de Riesgos y diseño de controles para Entidades Públicas diciembre 2020. DAFP

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

Análisis y evaluación de los controles – Atributos**:** A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla se puede observar la descripción y peso asociados a cada uno así:

Atributos de para el diseño del control:

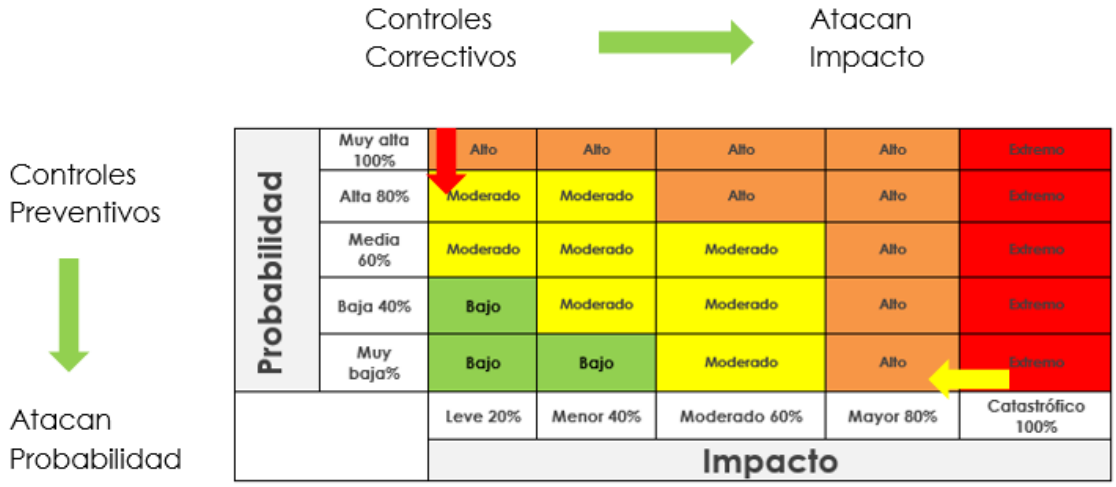
Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25 %
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15 %
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10 %
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la Intervención de personas para su realización.	25 %
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15 %
*Atributos informativo	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Guía de administración de Riesgos y diseño de controles para Entidades Públicas diciembre 2020. DAFP

***Nota:** Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor presentada anteriormente, se muestra en la imagen a continuación cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Movimiento en la matriz de calor acorde con el tipo de control:



En la siguiente tabla se observa la aplicación de la tabla de atributos, como ejemplo para el análisis y valoración de controles

Tabla de aplicación atributos de los controles

Características				Peso
Control 1	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con registro	x	-

Características				Peso
		Sin registro		-
Total valoración Control 1				**40%**
Control 2	Tipo	Preventivo		
		Detectivo	x	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con registro	x	-
		Sin registro		-
Total valoración Control 2				**30%**

Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante, luego de la aplicación del primer control.

Para mayor claridad, en la siguiente tabla se da continuación al ejemplo anterior, donde se observan los cálculos requeridos para la aplicación de los controles.

Tabla de aplicación de controles para establecer el riesgo residual.

Riesgo	Datos relacionaos con Probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Nombre del Riesgo	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad residual	25.2%			

	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Inherente	80%			

Riesgo	Datos relacionaos con Probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Nombre del Riesgo	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad residual	25.2%			
	Impacto Inherente	80%	Valoración control 1 preventivo		
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Inherente	80%			

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

La evaluación de todos los controles se realizará en la Matriz de Riesgos Institucional por proceso en el SGI Almera.

Debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, el responsable del proceso debe llevar a

cabo una confirmación, lo que posteriormente puede ser validado con las actividades de evaluación realizadas por auditoría interna o control interno.

Nivel del riesgo por proceso

Para determinar el nivel del riesgo por cada proceso, se identifica en la totalidad de los riesgos identificados para cada uno la MODA, la cual estadísticamente se entiende como el nivel de riesgo que más se repite en el proceso y este corresponde al Nivel del proceso.

Ejemplo:

Proceso X: tiene 9 riesgos calificados así:

BAJO BAJO MEDIO MEDIO MEDIO MEDIO MEDIO ALTO ALTO

En este caso la moda es el nivel medio

Si llega a presentarse que algunas frecuencias de niveles sea la misma y no exista una sola Moda, se determina por el nivel de riesgo más alto que se encuentre en el proceso entre las dos modas, con el fin de no perder de vista los riesgos más críticos asociados, los cuales serán objeto de intervención y seguimiento.

Ejemplo:

Proceso Y: tiene 9 riesgos calificados así:

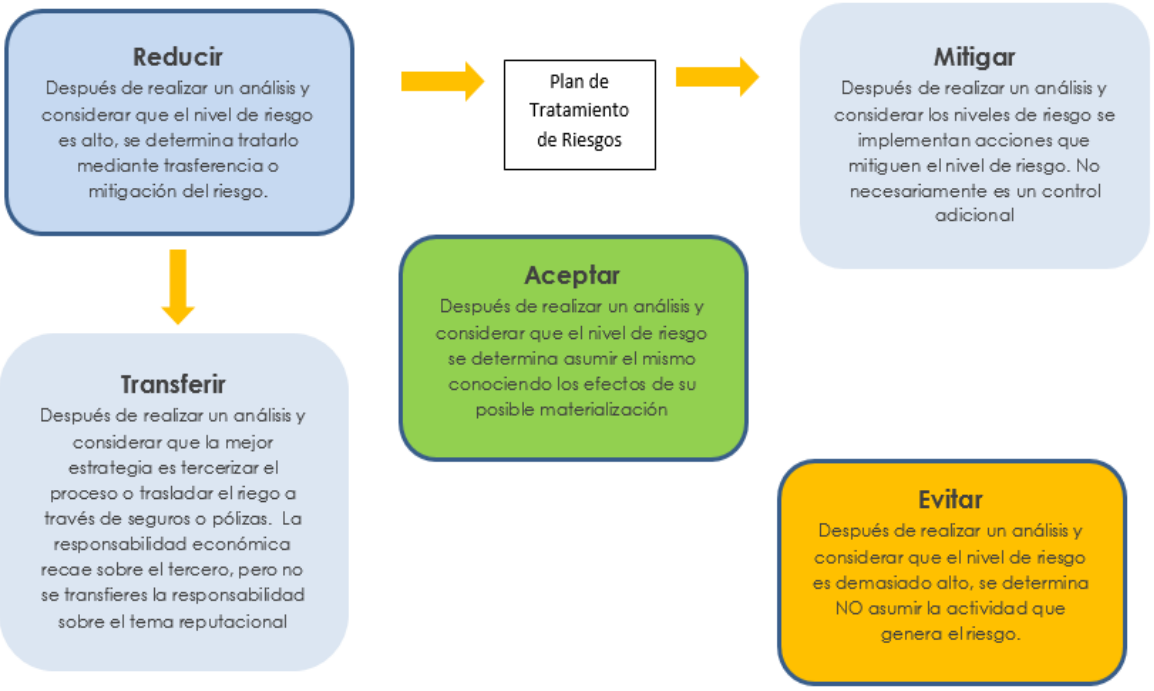
BAJO BAJO BAJO BAJO MEDIO ALTO ALTO ALTO ALTO

En este caso que hay dos modas, Bajo y Alto, se determina el proceso en nivel Alto.

8.2.3 Tratamiento del riesgo. Estrategias para combatir el riesgo.

Es la decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. **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 figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción o tratamiento de riesgos, dentro del respectivo mapa de riesgos



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, que en la empresa se denomina Plan de Tratamiento de Riesgos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción o tratamiento de riesgos, que especifique: responsable, fecha de implementación y fecha de seguimiento.

Nota: El plan de acción o de tratamiento de riesgos acá referido es diferente a un plan de contingencia, el cual se consideraría un control correctivo.

El tratamiento de los riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. En caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables definidos en la empresa, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción y lavado de activos y financiación del terrorismo la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías, no necesariamente excluyentes o apropiadas en todos los casos.

Acorde la aceptabilidad del riesgo, se establece el tratamiento del mismo, como se muestra en la siguiente tabla.

Nivel del riesgo	Nivel de aceptabilidad	Tratamiento
Extremo	**Inaceptable.**	**Evitar, reducir, compartir**
Alto	**Grave.**	**Evitar, reducir, compartir**
Moderado	**Tolerable.**	**Reducir**
Bajo	**Aceptable.**	**Aceptar**

A: Aceptar o Asumir el riesgo. **R**: reducir el riesgo **E**: Evitar riesgo. **C**: Compartir o Transferir el riesgo

8.3 MONITOREO, SEGUIMIENTO Y EVALUACIÓN DEL SISTEMA DE GESTIÓN DE RIESGO

El seguimiento y la evaluación del sistema se realizarán a través de las siguientes actividades:

- Seguimiento a la gestión de riesgos de la organización mediante la autoevaluación frente a criterios de la NTC ISO 31000.
  Se aplica anualmente una autoevaluación de cumplimiento en la Norma NTC ISO 31000, verificando su grado de implementación en Metrosalud como punto inicial para establecer el cronograma de trabajo y darle continuidad. Esta autoevaluación se lleva a cabo por el equipo de la Oficina Asesora de Planeación y Desarrollo Organizacional en el SGI Almera y se tienen en cuenta los criterios de valoración establecidos para la valoración de todos los sistemas en este aplicativo.
- Seguimiento al cumplimiento del Plan de tratamiento de riesgos una vez este formulado en el SGI Almera y se presenta el seguimiento en la evaluación de Plan de acción acorde con la periodicidad definida para ello.
- Seguimiento al reporte de sucesos administrativos a la Mesa de Ayuda de Riesgos, para obtener datos sobre la ocurrencia de los eventos administrativos que se presenta y que son insumo para el análisis del mapa de riesgos
- Seguimiento a la implementación del SARLAFT con todos sus componentes, entre estos, la debida diligencia, reportes internos y externos y los informes de seguimiento a Junta Directiva.
- Seguimiento a la efectividad de los controles por parte de los responsables de su implementación desde el autocontrol primera línea de defensa, desde la Oficina Asesora de Planeación y Desarrollo Organizacional y desde la Oficina de Control Interno y Evaluación, como segunda y tercera línea de defensa respectivamente.

- Seguimiento a indicadores Sistema Gestión Riesgos:
  - Proporción de cumplimiento de la NTC ISO 31000.
  - Proporción de cumplimiento en la ejecución del plan de tratamiento de riesgos
  - Cobertura en la capacitación de riesgos
  - Variación en el reporte de sucesos administrativos

Adicionalmente se incluyen algunos indicadores trazadores de los procesos, como Indicadores Clave de riesgos o KRI (Key Risk Indicator), a los cuales se les hará seguimiento acorde con lo definido en la ficha técnica de cada uno en el SGI Almera, por parte de los líderes de cada proceso. Estos indicadores se encuentran en el Anexo 1 de este documento y pueden ser objeto de modificación acorde con la dinámica de la empresa y sus procesos.

Se presentan los avances y resultados de la gestión de riesgos periódicamente al Comité Institucional de Gestión y Desempeño en el marco del seguimiento a la implementación del MIPG, al Comité de Coordinación de Control Interno como parte de su plan de trabajo y como se mencionó anteriormente en la evaluación de Plan de Acción. Adicionalmente se presenta informe de SARLAFT a Junta Directiva, quién debe emitir su concepto frente al informe presentado con el respectivo registro en el acta.

8.4 MEJORAMIENTO DEL SISTEMA DE GESTIÓN

8.4.1 Plan de mejora del sistema de gestión de riesgos

A partir de los resultados obtenidos anualmente en la autoevaluación, se genera desde la Oficina Asesora de Planeación y Desarrollo Organizacional el respectivo informe y acorde con los hallazgos obtenidos, se formula el Plan de Mejora en el SGI Almera y a través de este se realiza el seguimiento a su cumplimiento.

8.4.2 Aprendizaje Organizacional

A partir de los resultados de la autoevaluación, de los indicadores del sistema y de las situaciones presentadas en la vigencia del ciclo, se llevarán a cabo las mejoras requeridas en el sistema para el siguiente ciclo,

- **Comunicación**

El despliegue se realizará través de los medios institucionales definidos formalmente y en la estrategia de Despliegue Institucional en todas las Unidades Administrativas, por parte de la Oficina Asesora de Planeación y Desarrollo Institucional, acorde con la programación de estos.

Adicionalmente podrán programarse otro tipo de actividades en cada vigencia para mejorar la apropiación de la gestión de riesgos en los servidores, según las actividades institucionales, como boletines electrónicos, capacitación y talleres con equipos de trabajo, entre otros. Para la actualización del Mapa de riesgos, se realizará capacitación en la metodología a utilizar, previo al inicio de esta actividad.

Se presentan por otro lado avances y resultados en la evaluación de Plan de Acción, con la periodicidad establecida para esta actividad.

9. GLOSARIO DE TÉRMINOS

Gestión del riesgo. Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

Riesgo.

- Efecto de la incertidumbre sobre los objetivos. NTC ISO 31000
- Efecto que se causa sobre el objetivo de las entidades, debido a eventos potenciales. DAFP

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.

Riesgo de Corrupción. Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado

Parte interesada. Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

Factores o fuentes de Riesgo:

- Elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgo. NTC ISO 31000
- Son las fuentes generadoras de riesgos DAFP

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

Causa Inmediata. Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

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.

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.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

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

Control: Medida que permite reducir o mitigar un riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

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

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.

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.

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

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.

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.

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.

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.

SGI: Sistema de Gestión Integral, hace referencia al aplicativo para la gestión del mapa de riesgos, Almera.

IPS: Instituciones Prestadoras de Servicios de Salud

UPSS: Unidades Prestadoras de Servicios de Salud

10. BIBLIOGRAFÍA

Abecé Circular Externa 09 De 2016 – Implementación del SARLAFT. Superintendencia nacional de Salud y Ministerio de Salud

Circular 009 de 2016 Superintendencia Nacional de Salud

Circular externa 004 de 2018 Superintendencia Nacional de Salud

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 5. Departamento Administrativo de la Función Pública. Diciembre 2020.

Guía para la Gestión de Riesgos de Corrupción 2011. Presidencia de la República

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

NTC ISO 31000 2018. Gestión del riesgo. Icontec

11. DOCUMENTOS RELACIONADOS:

- Formato de Matriz de Riesgos SGI Almera
- Formato Plan de tratamiento de riesgos SGI Almera
- Manual SARLAFT

ELABORADO POR:	
Nombre: Natalia Peláez Miyar	Cargo: Profesional Especializada, Oficina Asesora Planeación y Desarrollo Organizacional
Nombre: Luz María Ramírez Correa	Cargo: Jefe Oficina Asesora Planeación y Desarrollo Organizacional

CONTROL DE ACTUALIZACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO O AJUSTE	RAZÓN DEL CAMBIO O AJUSTE	RESPONSABLE DEL CAMBIO O AJUSTE
01	15/06/2021	Actualmente se cuenta con el programa de gestión de riesgos: PE02 PG 150PROGRAMA GESTIÓN DE RIESGOS, el cual se debe eliminar para crear el Sistema de Gestión de Riesgos.	De conformidad con el nuevo plan de desarrollo, se define el proyecto desarrollo del Sistema Integrado de Gestión, en este se establece la necesidad de homologar los diferentes sistemas de gestión bajo un mismo esquema. El esquema tomado como referencia para realizar la homologación de los sistemas de gestión es el esquema de alto nivel de las normas ISO. El documento presentado se ajusta a estos estándares definidos. Adicionalmente se da inicio a un nuevo ciclo y se cuenta con una actualización de la Guía de Gestión de Riesgos y Diseño de controles del DAFP en diciembre de 2020.	Jefe Oficina Asesora Planeación y Desarrollo Organizacional