



POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO SANATORIO DE CONTRATACIÓN ESE

Contratación Santander, septiembre de 2026

CONTENIDO

1.	POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO	7
1.1.	Definición Política para Gestión Integral del Riesgo.....	7
1.2.	Alcance	7
1.3.	Tipologías de Riesgo a Gestionar.....	7
1.4.	Principios Orientadores.....	8
2.	MARCO LEGAL	9
3.	ESTABLECIMIENTO DEL CONTEXTO ESTRATÉGICO Y POR PROCESOS.....	11
3.1.	Contexto Externo e Interno	11
3.2.	Contexto por Proceso.....	12
4.	MANUAL DE GESTIÓN INTEGRAL DEL RIESGO	13
4.1.	Objetivo General	13
4.2.	Objetivos Específicos.....	13
4.3.	Estructura para la Gestión del Riesgo.....	13
4.4.	Términos y Definiciones.....	14
4.4.1.	Conceptos Clave Generales para la Gestión del Riesgo.....	14
4.4.2.	Conceptos Clave para la Gestión Preventiva del Riesgo Fiscal	15
4.4.3.	Conceptos Clave para la Gestión de Riesgos de Seguridad de la Información	16
4.4.4.	Conceptos Clave para la Gestión de Riesgos a la Integridad Pública	16
4.4.5.	Conceptos Clave para la Gestión de Riesgos en Sector Salud	19
4.5.	Metodología.....	21
4.6.	Responsabilidad Frente a la Gestión del Riesgo de Acuerdo con el Esquema de Líneas de Defensa	22
4.7.	Lineamientos para Riesgos Generales de Gestión	23
	Paso 1: Identificación y descripción del riesgo	23
4.7.1.	Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados	23

4.7.2.	Identificación de áreas de impacto	24
4.7.3.	Identificación de áreas de factores de riesgo	24
4.7.4.	Descripción del riesgo	25
Paso 2: Análisis de Riesgo Inherente.....		26
4.7.5.	Determinar la probabilidad.....	26
4.7.6.	Determinar el impacto	27
4.7.7.	Análisis de severidad	27
Paso 3: Diseño y Análisis de Controles.....		28
4.7.8.	Estructura para la Descripción del Control	28
4.7.9.	Tipologías de Controles	30
4.7.10.	Valoración de Controles.....	31
4.7.11.	Aplicación de Controles en la matriz de severidad	32
Paso 4: Valoración de Riesgo Residual.....		33
4.7.12.	Estrategias para combatir el riesgo	34
4.7.13.	Consolidación Mapa de Riesgos Integral.....	35
4.8.	Gestión Preventiva de Riesgos Fiscales	36
4.8.1.	Control fiscal interno y prevención del riesgo fiscal	36
4.8.2.	Definición y elementos del riesgo fiscal.....	37
4.8.3.	Metodología para el levantamiento del mapa de riesgos fiscales	37
Paso 1: Identificación de riesgos fiscales.....		37
Paso 2: Valoración del riesgo fiscal		42
Paso 3: Valoración de controles		42
4.9.	Riesgos de Seguridad de la Información.....	43
Paso 1: Identificación y descripción de riesgos de seguridad de la información		43
4.9.1.	Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados.	43
4.9.2.	Identificación de áreas de impacto	49

4.9.3. Identificación de áreas de factores de riesgo	49
4.9.4. Descripción del riesgo	52
Paso 2: Análisis de Riesgo Inherente	52
4.9.5. Determinar la probabilidad.....	53
4.9.6. Determinar el impacto	53
4.9.7. Análisis de severidad	54
Paso 3: Diseño y Análisis de Controles.....	55
4.9.8. Estructura para la Descripción del Control	55
4.9.9. Valoración de Controles.....	55
Paso 4: Valoración de Riesgo Residual.....	56
4.10. Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP	58
4.10.1. Integridad pública.....	58
4.10.2. Amenazas para la integridad pública	59
4.10.2.1.Soborno	59
4.10.2.2.Fraude	60
4.10.2.3.Inadecuada gestión del conflicto de intereses	60
4.10.2.4.Corrupción	60
4.10.2.5.Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP.....	61
4.10.3. Sistema de Gestión del Riesgo	61
4.10.3.1.Contexto de la organización.....	62
4.10.3.2.Liderazgo del Sistema	63
4.10.3.3.Planificación	64
4.10.3.4.Apoyo.....	65
4.10.3.5.Operación	66
4.10.3.5.1. Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos	67

Paso 1:	<i>Identificación y descripción del riesgo.....</i>	68
Paso 2:	<i>Análisis de Riesgo Inherente</i>	72
Paso 3:	<i>Diseño y Análisis de Controles.....</i>	73
Paso 4:	<i>Valoración de Riesgo Residual.....</i>	73
4.10.3.5.2.	Debida diligencia en el conocimiento de las contrapartes.....	73
4.10.3.5.3.	Función de cumplimiento.....	80
4.10.3.5.4.	Herramientas de gestión del riesgo.....	83
4.10.3.6.	Monitoreo, evaluación, auditoría y mejora	84
4.11.	Articulación de la Gestión del Riesgo para Entidades Públicas vigiladas por la Superintendencia Nacional de Salud.....	85
4.12.	Seguimiento, Monitoreo y Revisión en el marco del Esquema de Líneas del Modelo Estándar de Control Interno MECI.....	87
4.12.1.	Tipologías de Indicadores para el seguimiento	87
4.12.2.	Alcance de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI).....	90
4.12.3.	Lineamientos generales para el establecimiento de Indicadores clave de riesgo (KRI) 90	
4.12.4.	Comunicación y reporte KRI en el marco del esquema de líneas de aseguramiento	95
REFERENCIAS.....		98

INTRODUCCIÓN

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales, tanto públicas como privadas, la cual cobra mayor importancia dada la globalización y el cambio constante generado por la tecnología. Estos cambios hacen que las entidades se enfrenten a factores internos y/o externos, que pueden crear incertidumbre sobre el logro de los objetivos planteados.

El Sanatorio de Contratación ESE, comprometido con la calidad en la prestación del servicio de salud integral a los enfermos de Hansen y sus convivientes, así como a la población del municipio de Contratación y su área de influencia, implementará una Política de Integral del Riesgo, que permita controlar aquellos que puedan impedir el logro de los objetivos y procesos institucionales, identificándolos, evaluándolos y estableciendo las acciones a llevar a cabo para su prevención.

La elaboración de la Política de Administración del Riesgo del Sanatorio de Contratación ESE, se basó en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, expedida por el Departamento Administrativo de la Función Pública (DAFP) en agosto de 2025, la cual tiene como fin unificar los lineamientos en los aspectos comunes de las metodologías para la administración de los riesgos, fortalecer el enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos, así como la incorporación de los lineamientos para la identificación y tratamiento de los riesgos a la integridad pública, de acuerdo con el componente programático denominado Estrategia Institucional para la Lucha Contra la Corrupción.

1. POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO

El Sanatorio de Contratación ESE, se compromete a mantener bajo control los riesgos generales de gestión, fiscales, de seguridad de la información, para la integridad pública y los establecidos para las entidades vigiladas por la Superintendencia Nacional de Salud, mediante la aplicación del manual y metodología institucional. A través de controles preventivos y detectivos oportunos, la entidad busca evitar que las amenazas se concreten, corregir desviaciones y minimizar cualquier impacto negativo en sus diferentes procesos, para salvaguardar la integridad institucional.

1.1. Definición Política para Gestión Integral del Riesgo.

El Sanatorio de Contratación ESE adopta la Política de Gestión Integral del Riesgo, como una práctica preventiva, estratégica y transversal, integrada orgánicamente en sus procesos de planeación, gestión y evaluación, orientada a blindar la misión institucional y asegurar la prestación oportuna, humana y eficiente de los servicios de salud a sus usuarios y grupos de valor.

Esta política establece el compromiso de la Alta Dirección y de todos los servidores públicos y contratistas de la entidad para identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales. La gestión del riesgo en el Sanatorio de Contratación ESE, deja de ser un requisito formal de control para constituirse en un componente clave para la toma de decisiones informadas, la generación de valor público, la defensa jurídica preventiva, la optimización de los recursos y la salvaguarda de la confianza ciudadana, bajo los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).

1.2. Alcance

Esta política es vinculante y de aplicación obligatoria para todos los procesos institucionales (estratégicos, misionales, de apoyo y de evaluación y control), planes, programas, proyectos, y para las acciones ejecutadas por los servidores públicos y contratistas del Sanatorio de Contratación ESE en el desarrollo de sus funciones.

1.3. Tipologías de Riesgo a Gestionar

En consonancia con la Versión 7 de la Guía del DAFP, el Sanatorio administrará el riesgo bajo un enfoque integral que unifica criterios para las siguientes tipologías específicas:

- a. Riesgos Estratégicos: Eventos que impactan directamente el direccionamiento y las metas de largo plazo de la ESE.
- b. Riesgos Operativos: Fallas o deficiencias asociadas al talento humano, deficiencias en los procesos de salud o administrativos, tecnología e infraestructura.
- c. Riesgos de Integridad Pública (Corrupción): Conductas que desvíen la finalidad de la función pública para obtener beneficios particulares, articulados con el Plan de Transparencia y Ética Pública.
- d. Riesgos de Seguridad Digital (Seguridad de la Información): Amenazas y vulnerabilidades tecnológicas que pongan en peligro los activos de información, historias clínicas y datos sensibles de los usuarios (en articulación con MinTIC).
- e. Riesgos Fiscales: Situaciones que puedan generar impactos negativos y detrimento de los recursos financieros y patrimoniales de naturaleza pública asignados a la institución.
- f. Riesgos Emergentes: Identificación de nuevas amenazas relacionadas con la transformación digital, ciberseguridad, sostenibilidad ambiental y cambios en el entorno de la salud pública.
- g. Riesgo en salud: Concebido como el impacto negativo, de un suceso adverso en los determinantes sociales, ambientales y económicos, que actúan sobre el bienestar individual o colectivo, alterando la expectativa de vida saludable en las poblaciones afectadas y de influencia de la Entidad.

1.4. Principios Orientadores

En armonía con el Marco del COSO-ERM 2017 y la Gestión Integral del Riesgo en las Entidades Públicas, esta política se orienta en:

- a. Enfoque Preventivo y Proactivo: Priorización de acciones tendientes a evitar o mitigar la probabilidad de ocurrencia e impacto de los riesgos antes de su materialización.
- b. Cultura del Riesgo (Gobierno y Autocontrol): Promoción de la autoevaluación donde cada líder de proceso y su equipo actúan como la primera línea de defensa para identificar y reportar desviaciones.
- c. Definición del Apetito del Riesgo: Establecimiento formal de los niveles de aceptación y tolerancia al riesgo que la junta directiva y la gerencia están dispuestas a asumir en la búsqueda de sus objetivos.

2. MARCO LEGAL

El riesgo y su administración están fundamentados en el siguiente marco normativo:

Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones, artículo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan y literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Ley 489 de 1998, Estatuto Básico de Organización y funcionamiento de la administración Pública.

Ley 610 de 2000, por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.

Ley 1474 de 2011, Estatuto Anticorrupción. Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar estos riesgos, las estrategias Anti trámites y los mecanismos para mejorar la atención al ciudadano. Decreto 2641 del 17 de diciembre del 2012, por el cual se reglamenta los artículos 73 y 76 de la Ley 1474 de 2011.

Decreto 2641 de 2012, “Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011”: ARTÍCULO 1. Señálese como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”.

Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 1083 de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”: CAPÍTULO 5 “Elementos técnicos y administrativos que

fortalezcan el Sistema de Control Interno en las entidades y organismos del Estado”, ARTÍCULO 2.2.21.5.4 “Administración de riesgos”. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

Decreto 648 de 2017, “Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública”: SECCIÓN 2 “Protección Especial” ARTÍCULO 2.2.21.1.6 “Funciones del Comité Institucional de Coordinación de Control Interno”. Literal g. Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

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”: TÍTULO 23 Articulación del Sistema de Gestión con los Sistemas de Control Interno. ARTÍCULO 2.2.23.2. “Actualización del Modelo Estándar de Control Interno”. La actualización del Modelo Estándar de Control Interno para el Estado Colombiano – MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5 de la Ley 87 de 1993.

Decreto 403 de 2020, por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.

Ley 2195 de 2022, por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.

3. ESTABLECIMIENTO DEL CONTEXTO ESTRATÉGICO Y POR PROCESOS

El contexto estratégico permite de manera identificar apropiadamente de los riesgos, dado que se precisan los objetivos institucionales y los objetivos de los procesos, y como se lograrán.

Por lo tanto, partiendo de la dimensión del Direccionamiento Estratégico y la Planeación en el cual se evalúan y determinan los factores internos y externos que interactúan con la gestión y la ruta a seguir para lograr los objetivos, también provee información relevante y otorga la articulación debida a la Administración de Riesgos para desarrollar acciones sobre las situaciones que están impactando o pueden impactar los resultados. Adicionalmente, el contexto de los procesos dentro de la cadena de valor permite en mayor detalle establecer escenarios de riesgo y niveles de exposición que pueden afectar el normal desarrollo de actividades y que si no se atienden pueden generar impactos mayores.

La gestión de riesgos es dinámica como lo son las organizaciones, de ahí la importancia de establecer un seguimiento estricto y periódico, así como, el análisis de datos históricos, teóricos, opiniones de expertos, necesidades de cada proceso e incluso experiencias de otras entidades.

Con todo lo anterior, el Plan Estratégico Institucional y el modelo de gestión por procesos adaptado al MIPG son elementos fundamentales para asegurar desde el inicio la debida administración de riesgos.

Los líderes de los procesos y sus equipos deben tener en cuenta toda la información relacionada con el contexto estratégico y el contexto del proceso para las etapas de identificación y valoración de los riesgos.

3.1. Contexto Externo e Interno

Se determinan las características o aspectos esenciales del entorno en el cual se encuentra la Entidad, así como, los aspectos sobre los cuales la organización busca alcanzar sus objetivos. En esta etapa se pueden observar instrumentos como el Análisis DOFA o PESTEL y se obtienen los objetivos estratégicos y metas institucionales. En otras palabras, los elementos que constituyen el direccionamiento estratégico.

Dentro del análisis se pueden considerar los siguientes factores según corresponda:

Contexto	Factores	Descripción
Externo	Económicos	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia
	Políticos	Cambios de Gobierno, legislación, políticas públicas, regulación
	Sociales	Demografía, responsabilidad social, orden público.
	Tecnológicos	Avances en tecnología, acceso a los sistemas de información externos, gobierno digital.
	Medioambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Comunicación externa	Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.
Interno	Financieros	Presupuesto de funcionamiento y de inversión, infraestructura, capacidad instalada.
	Personal	Competencia de personal, estructura organizacional, funciones, responsabilidades, rotación, disponibilidad de personal, seguridad y salud, ocupaciones, cultura organizacional-
	Tecnología	Integridad, confiabilidad, sistemas de información y seguridad de información, flujos de información y proceso para la toma de decisiones, desarrollo, mantenimientos de los sistemas de producción.
	Estratégicos	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo, políticas y objetivos estratégicos.

Fuente: Direccionamiento Estratégico

3.2. Contexto por Proceso

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. En esta etapa se deben considerar los documentos de los procesos, su caracterización, procedimientos y todos aquellos que permiten conocer el qué, cómo, por qué y quién realiza las actividades de gestión y de control propias.

La caracterización de los procesos provee los aspectos principales que rodean al proceso, el objetivo, insumos, actividades y productos que es donde se pueden generar los riesgos que impactan la cadena de valor de la entidad. Se pueden considerar factores como:

Factores	Descripción
Diseño del Proceso	Claridad en la descripción del objetivo y alcance del proceso.
Interacción con otros procesos	Relación con otros procesos en cuanto a insumo, proveedores, productos, usuarios y clientes.
Transversalidad	Proceso que determina los lineamientos necesarios para el desarrollo de todos los procesos.
Procedimientos documentados	La pertinencia de los procesos que se desarrollan.
Líder del proceso	Grado de responsabilidad de los funcionarios frente al proceso.
Comunicaciones entre los procesos	Efectividad de los flujos de información determinado en la interacción de los procesos.

Fuente: Modelo de Gestión por procesos.

4. MANUAL DE GESTIÓN INTEGRAL DEL RIESGO

4.1. Objetivo General

Establecer los elementos y marco general para el control y la gestión del riesgo del Sanatorio de Contratación ESE, que permita a los funcionarios identificar, analizar, valorar, controlar y comunicar los riesgos, que crean incertidumbre en el logro de los objetivos propuestos en cada proceso, en concordancia con el Modelo Integrado de Planeación y Gestión MIPG y a mejores prácticas internacionales de gestión del riesgo basadas en COSO-ERM (2017), definiendo las alternativas de acción, encaminadas a reducirlos y/o mitigarlos, dándoles un adecuado tratamiento.

4.2. Objetivos Específicos

- a. Generar una visión sistémica acerca de la administración y evaluación de los riesgos.
- b. Aumentar la probabilidad de alcanzar los objetivos y proporcionar un aseguramiento razonable con respecto al logro de estos.
- c. Proteger los recursos del Sanatorio de Contratación ESE, resguardándolos contra la materialización de los riesgos.
- d. Concientizar la necesidad de identificar y tratar los riesgos en todos los niveles de la Entidad.
- e. Involucrar y comprometer a todos los servidores del Sanatorio de Contratación ESE, en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- f. Mejorar la eficacia y eficiencia operativa de la institución.
- g. Asegurar el cumplimiento normas, leyes y regulaciones.
- h. Identificar situaciones que, por sus características, pueden originar prácticas corruptas.

4.3. Estructura para la Gestión del Riesgo

Con el fin de ejercer una correcta Administración del Riesgo, el Sanatorio de Contratación ESE, adoptará la metodología propuesta por el Departamento Administrativo de la Función Pública DAFP, para la presente política, el marco de referencia será la “Guía para la Gestión Integral del Riesgo en entidades públicas, versión 7 (agosto de 2025)”.

El análisis integral de riesgo en el Entidad, involucra riesgos generales de gestión, riesgos fiscales, riesgos de seguridad de la información, riesgos para la integridad pública y riesgos para Entidades Públicas vigiladas por la Superintendencia Nacional de Salud

El resultado de aplicar la metodología propuesta será el mapa de riesgos por cada proceso, que integrará el Mapa de Riesgos Institucional, el cual a su vez consolidará los riesgos identificados, los recursos y acciones, encaminadas a mitigar los mismos y los responsables de su ejecución.

4.4. Términos y Definiciones¹

A continuación, se precisan las definiciones comunes a toda la gestión integral del riesgo, aplicables a las tipologías de riesgo específicas que se desarrollan en capítulos individuales dentro de la Guía para la Gestión Integral del Riesgo en Entidades Públicas v7, y que se relacionan en el anexo de la guía.

4.4.1. Conceptos Clave Generales para la Gestión del Riesgo

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **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.
- **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.
- **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.
- **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.
- **Punto de Riesgo:** Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

¹ Anexo 2 de la Guía para la Gestión Integral del riesgo en Entidades Públicas Versión 7. Función Pública. Dirección de Gestión y Desempeño Institucional agosto 2025

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

4.4.2. Conceptos Clave para la Gestión Preventiva del Riesgo Fiscal

- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:
 - a. **Bien de uso público:** aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.
 - b. **Bienes fiscales:** aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.
- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.
- **Patrimonio público:** Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).
- **Gestión del Riesgo Fiscal:** Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales.
- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la

recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)".

4.4.3. Conceptos Clave para la Gestión de Riesgos de Seguridad de la Información

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **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.

4.4.4. Conceptos Clave para la Gestión de Riesgos a la Integridad Pública

- **Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP:** esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.
- **Riesgos para la integridad:** Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas.
- **Soborno:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar. (A partir de ISO37001:2025)
- **Soborno entrante:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.

- **Soborno saliente:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad.
- **Fraude:** errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)
- **Conflicto de interés:** Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011)
- **Corrupción:** Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015)
- **Lavado de activos:** el artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien “adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades [relacionadas con un delito fuente], o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito”. El Lavado de Activos puede darse por: colocación, ocultamiento e integración.
- **Delito fuente:** según el artículo 323 de la Ley 599 de 2000, son delitos fuente del lavado de activos: tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, contrabando, contrabando

de hidrocarburos o sus derivados, fraude aduanero o favorecimiento y facilitación del contrabando, favorecimiento de contrabando de hidrocarburos o sus derivados, en cualquiera de sus formas.

- **Colocación:** es la disposición del dinero proveniente de actividades delictivas. Durante esta fase inicial, el determinador o autor introduce sus fondos ilegales en actividades legales o aparentemente legales, bien a través del sistema financiero o de otros tipos de negocios o contratos, tanto nacionales como internacionales.
- **Ocultamiento:** es la separación de fondos ilícitos de su fuente mediante una serie de transacciones, cuyo fin es desdibujar la transacción ilícita original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras para disimular el rastro documentado, la fuente y la propiedad de los fondos.
- **Integración:** es dar apariencia legítima a riqueza ilícita mediante el reingreso en la economía con transacciones comerciales o personales que aparentan ser normales. Esta fase conlleva la colocación de los fondos lavados de vuelta en la economía para crear una percepción de legitimidad. El lavador podría optar por invertir los fondos en bienes raíces, artículos de lujo o proyectos comerciales, entre otros.
- **Financiación del Terrorismo (FP):** el artículo 345 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien “directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas”. La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización.
- **Recaudación:** consiste en la búsqueda de fuentes de financiación por las organizaciones terroristas, bien sean de origen legal, como los aportes de los Estados, individuos, entidades, organizaciones y donantes en general que apoyan su causa o son engañados, así como recursos provenientes de cualquier actividad delictiva, fondos que generalmente circulan en efectivo.
- **Transmisión:** es la fase intermedia que busca poner el dinero recaudado a disposición de la organización terrorista, quedando simplemente la espera de su utilización final; corresponde al movimiento de los fondos a través de distintas técnicas, se trata de ocultar sus movimientos y destino final.
- **Utilización:** fase donde los fondos se utilizan básicamente para la financiación de la logística estructural de la organización o la logística operativa en materia de planeación y ejecución de actos terroristas.
- **Financiación de la Proliferación de Armas de Destrucción Masiva (FP):** fondos u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones

Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización.

- **Debida diligencia (due diligence):** proceso que deben llevar a cabo las entidades para identificar, prevenir, mitigar y explicar cómo abordan los impactos negativos reales y potenciales en sus propias actividades, su cadena de suministro y otras relaciones comerciales.
- **Debida diligencia en el conocimiento de la contraparte (debida diligencia del cliente):** proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera.
- **Función de cumplimiento:** función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.
- **Contraparte:** cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización.
- **Parte Interesada:** es un tipo de contraparte con la cual no se ha establecido ninguna relación o vínculo, pero que ha manifestado formalmente su interés en establecerlo.
- **Parte Vinculada:** para efectos del SIGRIP, es una contraparte dependiente de la organización con la cual se ha establecido una relación de especial de sujeción por su relación legal o reglamentaria, o laboral.
- **Parte Relacionada:** para efectos del SIGRIP, es una contraparte independiente de la organización con la cual se ha establecido una relación comercial, contractual o legal; o respecto de la cual se ejerce algún grado de control jerárquico, de tutela o de propiedad, sin detrimento de su independencia.

4.4.5. Conceptos Clave para la Gestión de Riesgos en Sector Salud

- **Riesgo en salud:** Es el efecto negativo que tiene un evento no deseado o cualquiera de los determinantes de la salud, sobre la salud de una persona o grupos de personas, y que usualmente implica un mayor uso de tecnologías en salud para su atención, o para mitigar sus consecuencias. Nota: Los determinantes de la salud se definen como “el conjunto de factores personales, sociales, económicos y ambientales que determinan la esperanza de vida saludable de los individuos y las poblaciones” (World Health Organization, 2021).

- **Sistema Integral de administración de riesgos de cumplimiento (SIARC):** Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por el máximo órgano social u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:
 - a. Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de riesgos asociados al LA/FT/FP, Corrupción, Fraude y de soborno transnacional. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.
 - b. Prevenir y mitigar la ocurrencia de riesgos asociados al LA/FT/FP, los actos de Corrupción, Fraudes y de soborno transnacional originados tanto al interior como al exterior de las organizaciones.
 - c. Realizar una gestión adecuada de los Riesgos.
- **Subsistema de Administración del Riesgo de Corrupción, Opacidad y Fraude – SICOF:** Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por el máximo órgano social u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:
 - a. Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de Corrupción, Opacidad y Fraude. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.
 - b. Prevenir y mitigar la ocurrencia de actos de Corrupción, Opacidad y Fraudes, originados tanto al interior como al exterior de las organizaciones.
 - c. Realizar una gestión adecuada de los Riesgos
- **Sistema General de Seguridad Social en Salud (SGSSS):** Sistema integrado por el Estado, a través del Ministerio de Salud y Protección Social, quien actúa como organismo de coordinación, dirección y control; las Entidades Promotoras de Salud (EPS), responsables de la afiliación y el recaudo de las cotizaciones y de garantizar la prestación del Plan Obligatorio de Salud a los afiliados; y las instituciones prestadoras de salud (IPS), que son los hospitales, clínicas y laboratorios, entre otros, encargadas de prestar la atención a los usuarios. También hacen parte del SGSSS las Entidades Territoriales y la Superintendencia Nacional de Salud. El SGSSS tiene como objetivo regular el servicio público esencial de salud y crear condiciones de acceso para toda la población residente del país, en todos los niveles de atención.
- **Sistema de Control Interno:** sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de

verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

- **Superintendencia Nacional de Salud (SUPERSALUD):** Entidad encargada de proteger los derechos de los usuarios del Sistema General de Seguridad Social en Salud mediante la inspección, vigilancia, control y el ejercicio de la función jurisdiccional y de conciliación, de manera transparente y oportuna.

4.5. Metodología

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Figura Metodología para la gestión del riesgo



4.6. Responsabilidad Frente a la Gestión del Riesgo de Acuerdo con el Esquema de Líneas de Defensa

El Modelo Integrado de Planeación y Gestión (MIPG) a través del Modelo Estándar de Control Interno (MECI) establece una estructura de control para la gestión institucional que determina los parámetros necesarios para la autogestión, la autorregulación y el autocontrol. Uno de los elementos fundamentales de esta estructura es el esquema de responsabilidades integrado por cuatro líneas de defensa el cual proporciona una manera efectiva para mejorar las comunicaciones en la gestión de los riesgos y los controles mediante la aclaración de las funciones y deberes relacionados.

En la siguiente tabla se explica la aplicación de los roles y responsabilidades del esquema de líneas de defensa para el Sanatorio de Contratación ESE

Responsabilidades de las líneas de defensa

Línea de defensa	Responsable	Responsabilidad frente a la gestión del riesgo
Línea estratégica	La Alta Dirección de la ESE (El Gerente y su Equipo Directivo) El Comité Institucional de Coordinación de Control Interno	Definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.
Primera línea de defensa	Líderes de procesos, programas y proyectos y sus equipos Los servidores públicos de todos los niveles de la ESE	Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo).
Segunda línea de defensa	Jefe de la Oficina de Planeación. Comité de compras. Encargado TIC Responsables de temas transversales para toda la entidad y que reporta ante el Representante Legal	Hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento

Línea de defensa	Responsable	Responsabilidad frente a la gestión del riesgo
		a los líderes de los procesos y sus equipos para la mejora de este tema.
Tercera línea de defensa	Oficina de Control Interno	A través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación.

Fuente: Basado en Guía para la Administración del Riesgo Versión 6, DAFP.

4.7. Lineamientos para Riesgos Generales de Gestión

Esta etapa tiene como propósito identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso y el análisis frente a los factores internos y externos, que pueden generar riesgos en el cumplimiento de los objetivos. Se aplican las siguientes fases:

Paso 1: Identificación y descripción del riesgo

4.7.1. Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados

Para este análisis, se debe tener en cuenta los siguiente:

- Análisis de objetivos estratégicos y de los procesos:** este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.
- Identificación de los puntos de riesgo:** son 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.

4.7.2. Identificación de áreas de impacto

El área 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.

4.7.3. Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la siguiente Tabla encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

Factores de riesgo

Factor	Definición	Descriptor
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos Falta segregación de funciones Errores de grabación, autorización Falta de supervisión o interventoría Errores en cálculos para pagos internos y externos Alta rotación o insuficiencia de personal Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo Acciones contrarias a las leyes o acuerdos contractuales Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas) Productos (bienes o servicios) que oferta/requiere Canales utilizados para la operación Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Fraude Interno Soborno Gestión inadecuada de conflicto de Intereses Corrupción Hurtos activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos Caída de sistemas de información y aplicaciones Caída de redes Errores en hardware o software Errores en programas

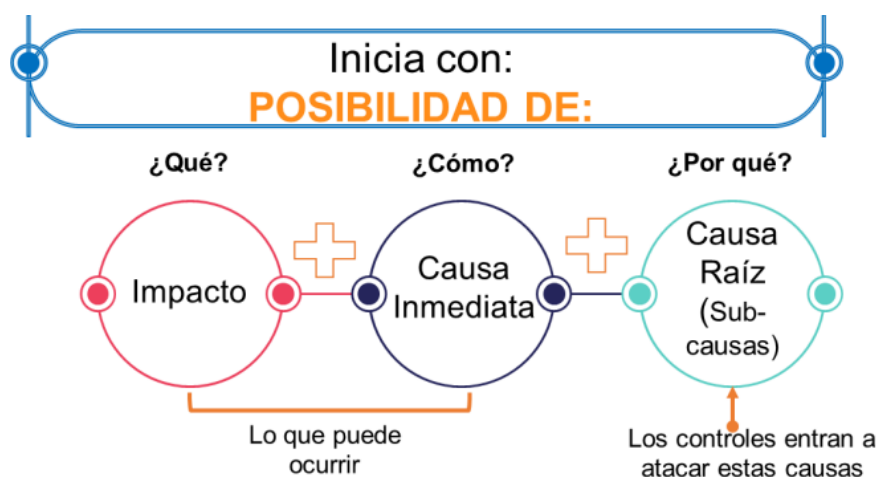
Factor	Definición	Descriptor
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes Incendios Inundaciones Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.	Fraude Externo Suplantación de identidad Asalto a la oficina Atentados, vandalismo, orden público

Fuente: Adaptado de la Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025.

4.7.4. Descripción del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Estructura propuesta para la redacción del riesgo



Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo. Desglosando la estructura propuesta tenemos:

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

- b. 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.
- c. 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 puede n existir más de una causa o subcausas que pueden ser analizadas.

Teniendo en cuenta lo anterior, una representación simplificada del modelo de descripción del riesgo contiene los siguientes elementos:

Evento no deseado y sus posibles consecuencias: ¿Qué puede pasar?

Causas: ¿Por qué puede pasar?

Tipología: ¿A qué categoría pertenece?

Factor de riesgo: ¿Qué condición aumenta su probabilidad?

Paso 2: Análisis de Riesgo Inherente

4.7.5. Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad:

Probabilidad	Frecuencia de la Actividad
Muy Baja - 20%	La actividad que conlleva se ejecuta el riesgo como máximo 2 veces al año
Baja - 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año
Media - 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta - 80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alto - 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFF, 2025.

4.7.6. Determinar el impacto

Son las consecuencias que puede ocasionar a la Entidad por la materialización de un riesgo. Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

En la siguiente tabla se establecen los criterios para definir el nivel de impacto.

Nivel de Impacto	Frecuencia de la Actividad	Frecuencia de la Actividad
Leve -20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la Entidad
Menor - 40%	Afectación mayor a 10 SMLMV y menor a 50 SMLMV	El riesgo afecta la imagen de la Entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o proveedores
Moderado - 60%	Afectación mayor a 50 SMLMV y menor a 100 SMLMV	El riesgo afecta la imagen de la Entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor - 80%	Afectación mayor a 100 SMLMV y menor a 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%	Afectación mayor a 500 SMLMV	El riesgo afecta la imagen de la Entidad con efecto publicitario sostenido a nivel país.

Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025.

4.7.7. Análisis de severidad

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 y a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar el nivel de RIESGO INHERENTE.

		Impacto				
Probabilidad	Muy Alto 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 20%	Bajo	Bajo	Moderado	Alto	Extremo
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025.

Paso 3: Diseño y Análisis de Controles

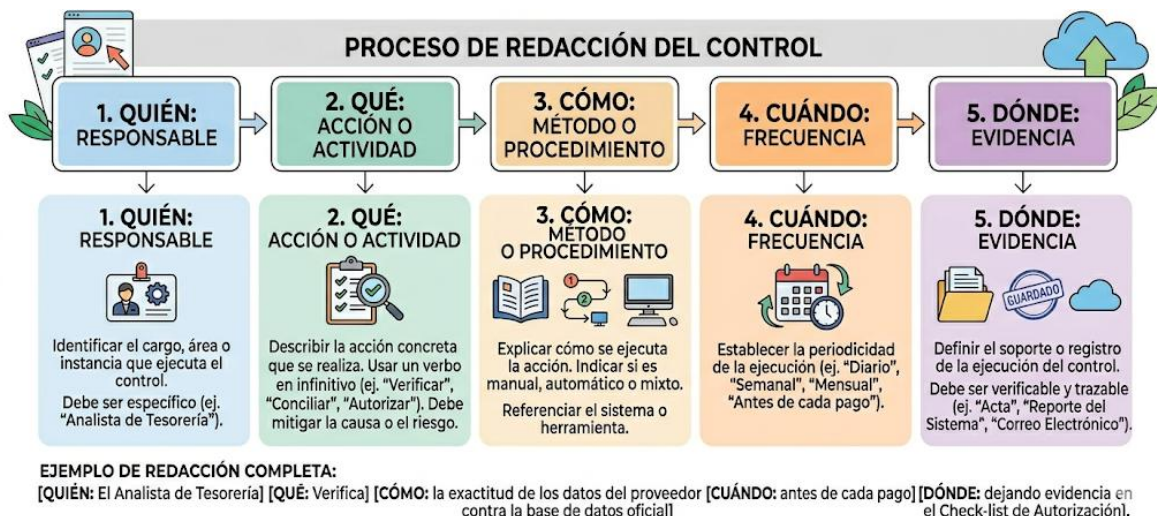
Las actividades de control son acciones concretas y con unos atributos específicos que son establecidas a través de políticas, procedimientos u otras directrices o documentos institucionales e implementadas con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos. Para la identificación o bien el diseño de controles se debe tener en cuenta que:

- Estas se pueden diseñar y establecer para cada riesgo a través de diferentes mecanismos, bien sea a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.
- Se requiere considerar los diferentes atributos de las actividades de control para asegurar aspectos tales como: los responsables de su ejecución, la segregación de funciones y niveles de autoridad apropiados.

4.7.8. Estructura para la Descripción del Control

Para un adecuado diseño de las actividades de control se propone una estructura para su redacción que agrupa los atributos necesarios para garantizar su implementación de forma efectiva por parte del responsable.

Desglosando la estructura propuesta tenemos el despliegue de los atributos para el control así: Responsable: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (Directores, asesores, profesionales, técnicos, asistenciales), así como su despliegue en



Fuente: Adaptado de la Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025

Desglosando la estructura propuesta tenemos el despliegue de los atributos para el control así:

- Responsable: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (Directores, asesores, profesionales, técnicos, asistenciales), así como su despliegue en grupos de trabajo internos e incluir coordinadores o gerentes de proyectos. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.

Su definición deberá igualmente considerar que éste cuenta con un nivel de autoridad apropiado de cara a la actividad de control, así como aspectos básicos de segregación de funciones para evitar que quién sea la fuente generadora de riesgo, sea el único que aplica alguna actividad de control.

- Acción: Determina para qué se realiza el control, se utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.

c. Atributos Informativos o de formalización del control: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:

- Documentación: se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
- Frecuencia: corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
- Evidencia: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
- Ejecución: permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta.

4.7.9. Tipologías de Controles

Con el fin de establecer la tipología de controles para su posterior validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, detectivo o correctivo, o bien una combinación de estos.

Para comprender esta estructura conceptual, a continuación, se consideran desde la cadena de valor de los procesos, con el fin de establecer en qué momento se activa el control en función de las actividades clave del proceso, base para la definición de los controles aplicables en sus 3 tipologías que se explican a continuación.

- a. Control preventivo: 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.
- b. Control detectivo: accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- c. Control correctivo: accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Se debe tener en cuenta que los controles que se contemplan en esta tipología usualmente tienen que ver con pólizas de seguro, copias de seguridad (backup), bancos de datos u otros mecanismos que

permiten enfrentar el riesgo una vez materializado, los cuales se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización pero no pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad. En consecuencia, si bien estos controles requieren en su diseño que se apliquen actividades con un enfoque preventivo, al ser activados al momento de materialización del riesgo deben ser considerados como controles correctivos no preventivos.

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

- Control manual: ejecutados por personas.
- Control automático: ejecutados por un sistema o software previamente programado o diseñado.

4.7.10. Valoración de Controles

La valoración de controles determina la forma como se califican los atributos o características de Eficiencia.

Características de Eficiencia	Peso	
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025.

Todos los demás atributos informativos o de formalización del control, explicados en el acápite de Estructura para la Descripción del Control, no se aplica valoración, pero deben analizarse para garantizar su el diseño.

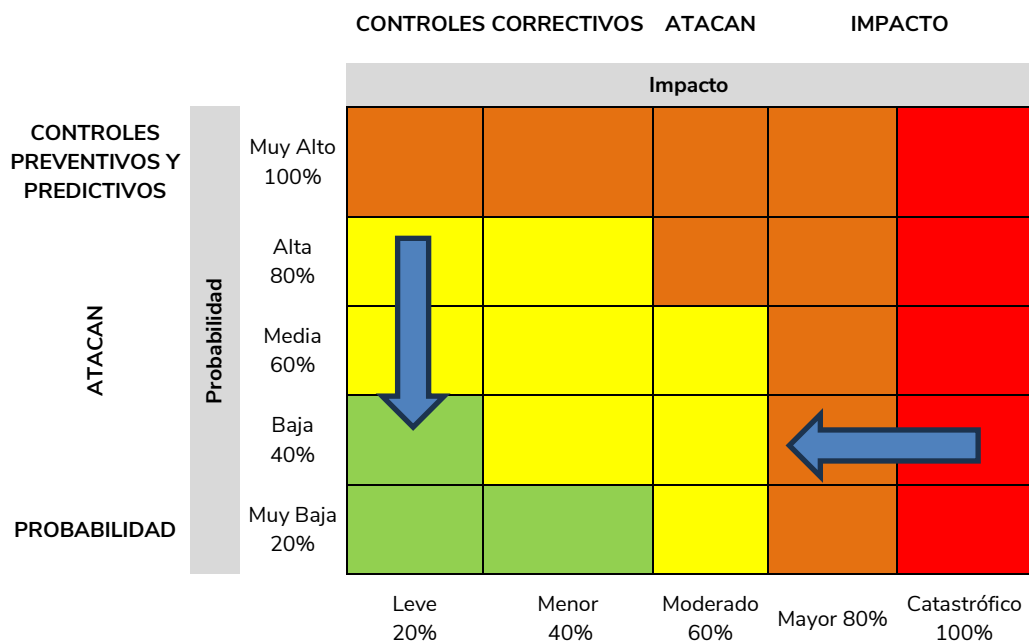
Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).

Características de Eficiencia		Descripción
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFF, 2025.

4.7.11. Aplicación de Controles en la matriz de severidad

Se debe tener en cuenta, que es a partir de los controles, que se dará el movimiento en la matriz de calor. A continuación, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFF, 2025.

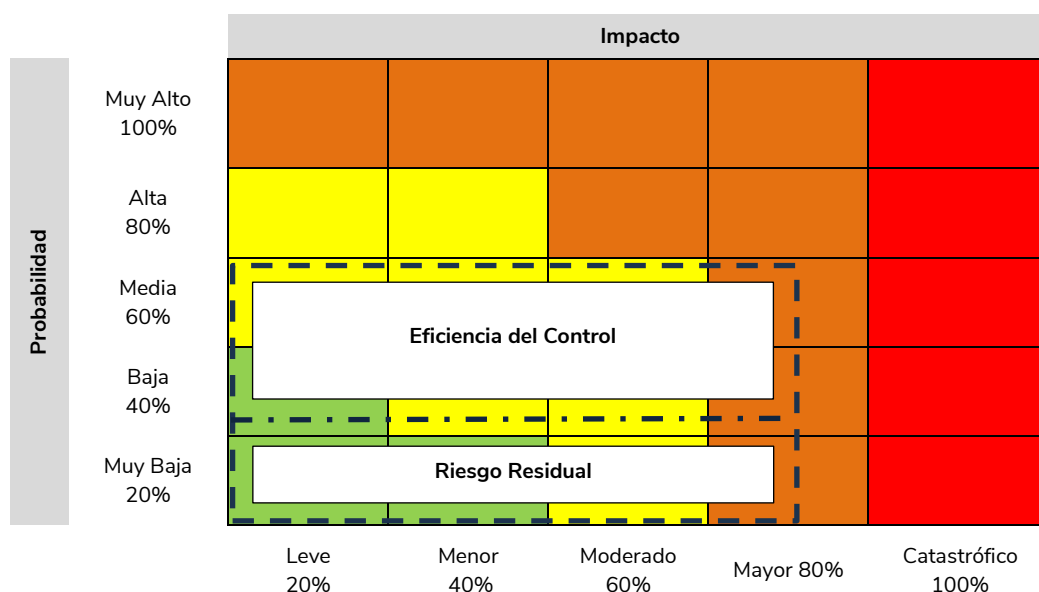
Paso 4: Valoración de Riesgo Residual

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.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes	Datos valoración de controles	Cálculos requeridos		
Posibilidad de pérdida económica multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Valoración de Probabilidad				
	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control			36%	
	Valoración control 2 detectivo			30%	36%*30%=10,8% 36%-10,8%=25,2%
	Probabilidad Residual			25,2%	
	Valoración de Impacto				
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual			80%	

Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025

Gráficamente el movimiento en la matriz de calor se muestra a continuación:



Fuente: Guía de Gestión para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, DAFP, 2025

4.7.12. Estrategias para combatir el riesgo

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.

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

En la siguiente figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.



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

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio² y se consideraría un control correctivo.

4.7.13. Consolidación Mapa de Riesgos Integral

A partir de la aplicación de cada uno de los pasos metodológicos ya explicados se procede con la elaboración y consolidación del mapa integral de riesgos, para lo cual se propone una matriz descriptiva, acompañada de un esquema gráfico que resume los análisis adelantados y permite contar con una visión integral de las diferentes tipologías de riesgos aplicables a cada proceso.

Es necesario tener en cuenta que los mapas de riesgos por proceso deben vincular las tipologías de riesgo aplicables, de acuerdo con las características de cada proceso, su complejidad, interacción con otros procesos, recursos, productos y servicios que gestiona, usuarios que atiende, bien sea internos o externos, con el fin de contar con mapas integrales.

² De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

4.8. Gestión Preventiva de Riesgos Fiscales

La finalidad es orientar el análisis de la operación de las entidades públicas para identificar y gestionar los riesgos que puedan provocar un daño patrimonial al Estado, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado. Para ello, es necesario partir del concepto de gestión fiscal, que incluye los siguientes componentes que se explican a continuación.

Concepto gestión fiscal – componentes

¿Qué es?	¿Quién la realiza?	¿Qué comprende?		¿Para qué?
El conjunto de actividades económicas, jurídicas y tecnológicas	Los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos	La adecuada y correcta adquisición planeación conservación administración custodia explotación enajenación consumo adjudicación gasto inversión disposición	De los bienes públicos	En orden a cumplir los fines esenciales del Estado, con sujeción a los principios establecidos en artículo 3 de la Ley 610 de 2000
		recaudación manejo inversión	De sus rentas	

Fuente: Elaboración Dirección de Gestión y Desempeño. 2025. Con base en Ley 610/2000 art. 3.

4.8.1. Control fiscal interno y prevención del riesgo fiscal

La construcción de este capítulo tiene como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

4.8.2. Definición y elementos del riesgo fiscal

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, este define riesgo fiscal, así:

“Efecto dañoso sobre los recursos públicos o bienes o interés patrimoniales de naturaleza pública, a causa de un **evento potencial**”

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento potencial (potencial conducta) + Efecto dañoso

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

4.8.3. Metodología para el levantamiento del mapa de riesgos fiscales

Paso 1: Identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas³.

³ Artículo 3 Ley 610 de 2000.

1.1 Puntos de riesgo y las circunstancias inmediatas

Los puntos de riesgo fiscal son eventos en los que potencialmente se genera riesgo fiscal, es decir, son las actividades propias de la gestión fiscal (, para lo cual es pertinente prestar especial atención a aquellas en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal. En cuanto a las circunstancias inmediatas son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo.

Por cada punto de riesgo, con frecuencia existen múltiples circunstancias inmediatas. La identificación de los puntos de riesgo y las circunstancias inmediatas han de ser el resultado del trabajo conjunto entre el personal directivo, asesor y demás servidores que por su experiencia o formación puedan aportar al análisis crítico y objetivo de la gestión fiscal de la entidad. Para la identificación, se pueden usar las siguientes preguntas orientadoras:

Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas

Preguntas y criterios para la identificación	Sirve para identificar
¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal)	Puntos de riesgo fiscal
¿Qué puntos de riesgo fiscal y circunstancias inmediatas del “¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” (anexo 1), son aplicables a la entidad?	Puntos de riesgo fiscal y circunstancias inmediatas
Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. En un ejercicio autocrítico, realista y objetivo, ¿cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual	Puntos de riesgo fiscal y circunstancias inmediatas

Preguntas y criterios para la identificación	Sirve para identificar
se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.	
En un ejercicio autocrítico, realista y objetivo, ¿cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.	Circunstancias inmediatas

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

1.2 Identificación de las áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Para definir de manera correcta el área de impacto, al momento de identificar y redactar riesgos fiscales, es fundamental tener claro el concepto de patrimonio público a partir de las tres expresiones que se derivan del artículo 6 de la Ley 610 de 2000:

Bienes públicos: Son todos aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público (aquellos cuyo uso pertenece a todos los habitantes del territorio nacional) y bienes fiscales (aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos).

Recursos públicos: Son los dineros comprometidos y ejecutados en ejercicio de la función pública.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

1.3 Identificar el efecto económico

El efecto económico del riesgo fiscal es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- a. Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
- b. Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público
- c. Multas impuestas por hechos que no comportan gestión fiscal
- d. Existencia de actuación de cobro coactivo por parte de la entidad.
- e. Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.
- f. Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su “normal uso” (máquinas eléctricas, computadores, celulares, etc.). (Contraloría General de la República, 2023, p. 12).

1.4 Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho

generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal (efecto dañoso).

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Al ser la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador. Es fundamental entonces, deslindar el hecho que ocasiona el daño (evento potencial o causa raíz), del daño propiamente dicho (efecto dañoso)

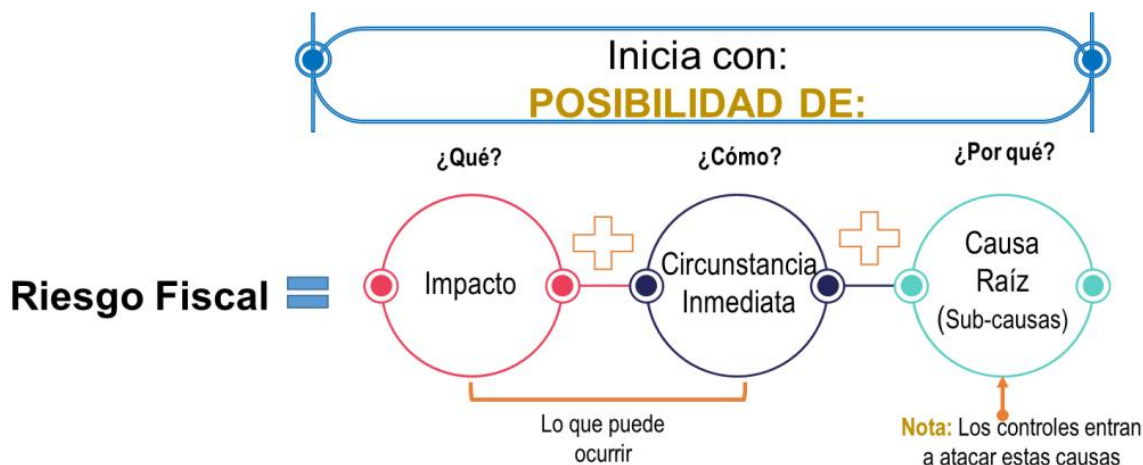
Descripción del Riesgo Fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales.

Para redactar un riesgo fiscal, se debe tener en cuenta:

- a. *Iniciar con la expresión:* Posibilidad de, dado que nos estamos refiriendo al evento potencial.
- b. *Impacto:* corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre el área de impacto (recursos públicos, bienes o intereses patrimoniales de naturaleza pública).
- c. *Circunstancia inmediata:* corresponde al cómo. Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera.
- d. *Causa Raíz:* corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño. Es la condición necesaria del riesgo, de tal forma que, si ese hecho no se produce, el daño no se genera.

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Paso 2: Valoración del riesgo fiscal

En esta etapa se realiza la Evaluación de riesgos que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto en la gestión fiscal.

Probabilidad: La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

Impacto: Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso recae sobre un bien, recurso o interés patrimonial de naturaleza pública. Toda potencial consecuencia económica sobre el patrimonio público, es relevante, sin embargo, existen niveles para su valoración.

Determinación del nivel de riesgo inherente: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad

Para la evaluación del riesgo fiscal, se aplicarán las tablas de frecuencia e impacto, así como la matriz de severidad, las cuales pueden adaptarse a las características propias de la entidad sin alterar los criterios de evaluación

Paso 3. Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Los controles pueden ser preventivos, detectivos o correctivos dependiendo el momento (antes, durante o después) en que se accionen respecto a la actividad que origina el riesgo fiscal (punto de riesgo). Los controles preventivos buscan asegurar que no se presente la causa raíz, los controles detectivos buscar tomar medidas ante la ocurrencia de la causa raíz para evitar que se produzca el efecto dañoso y los controles correctivos actúan ante el daño potencial, procurando detener su materialización o reparando el daño causado.

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

4.9. Riesgos de Seguridad de la Información

El objetivo de este capítulo es orientar a las entidades públicas del orden nacional y del sector público en general, en la implementación de un proceso de Gestión de Riesgos de Seguridad de la información, que permita incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades.

El Modelo de Seguridad y Privacidad de la Información es un instrumento desarrollado por el Ministerio de las Tecnologías de la Información y de las Comunicaciones que imparte los lineamientos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información basado en las normas y estándares de mejores prácticas en materia de seguridad de la información.

A continuación, se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la Disponibilidad, Integridad y Confidencialidad de los activos de información que permiten cumplir con la misión y alcanzar la Visión en las diferentes entidades.

Paso 1: *Identificación y descripción de riesgos de seguridad de la información*

4.9.1. Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados.

En primer lugar, se deben identificar los activos de Información⁷ mediante las actividades descritas en los “Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional” del MSPI, en esta se presenta los

lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación y clasificación de activos de información de cada entidad.

Para el diligenciamiento del inventario la entidad pública debe tener en cuenta los siguientes pasos, establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

- Paso 1. Listar los activos por cada proceso.
- Paso 2. Identificar el dueño y custodio de los activos
- Paso 3. Clasificar los activos por tipo (Hardware, software, etc)
- Paso 4. Clasificar la información
- Paso 5. Determinar la criticidad del activo
- Paso 6. Identificar si existe Infraestructuras Críticas Cibernéticas Nacionales

Se deben listar cada uno de los activos de información de la entidad que corresponden al alcance del proyecto, luego, para cada activo se deben registrar los siguientes datos:

Macroproceso: Macroproceso de la Entidad al que pertenece el activo de información (En caso de que existan).

Proceso: Proceso de la Entidad al que pertenece el activo de información.

Identificador: Se sugiere que el identificador sea una concatenación del código de la dependencia según la Tabla de Retención Documental (TRD) + número consecutivo.

Tipo: Define el tipo de Activo de Información:

- a. Información y datos de la entidad: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros
- b. Sistemas de información y aplicaciones de Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- c. Dispositivos de Tecnologías de información- Hardware: Equipos de cómputo que por su criticidad son considerados activos de información, no sólo activos fijos.
- d. Soporte para almacenamiento de información: Equipo para almacenamiento de información como USB, Discos Duros, CDs, SAN, NAS.
- e. Servicios: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- f. Recursos Humanos
- g. Instalaciones

h. Redes

Oficina: Área, dependencia o proceso que está identificando el activo de información.

Serie documental: Serie documental del área, dependencia o proceso que se encuentra identificando el Activo.

Subserie documental: Subserie documental del área, dependencia o proceso que se encuentra identificando el Activo.

Nombre: Nombre completo del activo de información.

Descripción: Descripción resumida de manera clara para identificar el activo de información. Nombre del responsable de la producción de la información (Propietario del activo): Nombre del área, dependencia, proceso responsable de producir el activo de información

Fecha de generación de la información: Fecha en la que el activo de información fue incluido en el inventario – TRD.

Nombre del responsable de la información (Custodio del activo): Corresponde al nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección.

Fecha de ingreso del activo al archivo: Fecha en la que el activo ingresa al archivo de gestión.

Soporte de registro: De acuerdo con el Decreto 2609 de 2012:

- a. Físico (análogo)
- b. Digital (electrónico) Este campo se diligencia si el Tipo de activo es "Información"
- c. N/A: Para el resto de los tipos de activos se debe seleccionar N/A.

Medio de conservación: De acuerdo con el Decreto 2609 de 2012 Archivo Institucional Es la instancia administrativa de custodiar, organizar y proteger.

Formato: Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: Hoja de cálculo, imagen, audio, video, documento de texto, etc.

Idioma: Establece el idioma, lengua o dialecto en que se encuentra la información.

A continuación, se realiza la Clasificación de Activos de Información de acuerdo con la propiedad correspondiente: Disponibilidad, Integridad y Confidencialidad.

Para cada activo se define el nivel de criticidad de la propiedad específica, para cada propiedad “se definieron tres (3) niveles que permiten determinar el valor general o criticidad del activo en la entidad”: Alta, Media y Baja, que corresponden con Criterios de Clasificación para cada una de las propiedades de la Información.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

El nivel de clasificación del activo corresponderá con el resultado de la sumatoria de la tabla de criterios de clasificación, que se muestra a continuación.

Niveles de clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Este resultado corresponde con el nivel de Criticidad del activo.

- **Es Infraestructura Crítica cibernética Nacional:** Se define si el activo corresponde con los criterios de Infraestructura Crítica cibernética descritos en los “lineamiento para la identificación de las infraestructuras críticas cibernéticas” del MSPI.
- **Información publicada:** Se define si el activo está publicado en la intranet, en internet o no está publicado.
 - a. Publicada: Si la información es publica y se puede consultar en un sitio web (interno o externo) o un sistema de información del Estado.
 - b. Publicada (Interno - Intranet)
 - c. Publicada (Externo - Internet)
 - d. No Publicada: Si la información se encuentra en la Entidad, pero no se encuentra en un sistema de información o sitio web.
- **Lugar de consulta o ubicación:** Indica la URL, sitio web o sistema de información donde puede ser consultada la información si esta se encuentra pública, el lugar de consulta si no está publicada o ubicación física.

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)						
Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	Es Infraestructura Crítica cibernética	Información publicada	Lugar de consulta o ubicación

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

El siguiente bloque corresponde con el Índice de información clasificada y reservada:

- **Objeto legítimo de la excepción:** La identificación de la excepción que, dentro de las previstas en los artículos 18 y 19 de la Ley 1712 de 2014, cubre la calificación de información reservada o clasificada. Si la respuesta es NO se debe marcar no aplica (N/A) en los demás campos sobre el índice de información clasificada y reservada.
- **Fundamento constitucional o legal:** Indica el fundamento constitucional o legal que justifica la clasificación o la reserva, señalando expresamente la norma, artículo, inciso o párrafo que la ampara.
- **Fundamento jurídico de la excepción:** Indica la norma jurídica que sirve como fundamento jurídico para la clasificación o reserva de la información.
- **Excepción total o parcial:** Según sea integral o parcial la calificación, las partes o secciones clasificadas o reservadas. Indicar si la totalidad del documento es clasificado o reservado o si solo una parte corresponde a esta calificación
- **Fecha de clasificación (DD/MM/AAAA):** Fecha en que se calificó la información como reservada o clasificada.
- **Tiempo de clasificación:** Tiempo que cubre la clasificación o reserva. La clasificación es ilimitada en años, la reserva solo puede durar como máximo por 15 años desde la creación del documento.

ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA (DECRETO 103 DE 2015)					
Objeto legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de clasificación (DD/MM/AAAA)	Tiempo de clasificación

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

El siguiente bloque corresponde con los activos de información que contienen datos personales:

- **¿Contiene datos personales?:** ¿El activo de información contiene datos personales? SI – NO

- **¿Contiene datos personales de niños, niñas o adolescentes?:** Son los datos personales de los niños, niñas y adolescentes, cuyo tratamiento está prohibido, salvo que se trate de datos de naturaleza pública. Ej. Registro civil.
- **Tipos de datos personales:** Si cuenta con datos personales seleccione el tipo, en caso contrario seleccione N/A:
 - a. Dato personal público: Toda información personal que es de conocimiento libre y abierto para el público en general. Ejemplo: Número de identificación apellidos.
 - b. Dato personal privado: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general. Ejemplo: Dirección de residencia y N° teléfono.
 - c. Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector y grupo de personas. Ejemplo: Fecha y lugar de nacimiento
- **Finalidad de la recolección de los datos personales:** La finalidad de la recolección justifica por la cual el dato es capturado, almacenado y mantenido en la Entidad
- **Existe la autorización para el tratamiento de los datos personales:** Seleccionar si se cuenta o no con la autorización de la recolección y tratamiento.

DATOS PERSONALES (LEY 1581 DE 2012)				
¿Contiene datos personales?	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Existe la autorización para el tratamiento de los datos personales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Importante: Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información por los líderes de los procesos, se debe enviar la matriz para su consolidación y validación por parte de la Oficina Asesora Jurídica para finalmente ser presentada ante el Comité Institucional de Gestión y Desempeño.

Finalmente se realiza el etiquetado de la información para que los usuarios puedan establecer el nivel de confidencialidad de cada documento.

El resultado de esta actividad es la Matriz del Inventario de Activos de Información que es el insumo principal para la Gestión de Riesgos de Seguridad de la Información proceso que se encuentra descrito en la Guía “Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas”.

Se debe establecer según el nivel de criticidad a cuáles activos se les realizará el correspondiente análisis de riesgos.

Matriz de Riesgos de Seguridad de la Información: Con base en la criticidad se realiza el proceso de gestión de riesgos, la cual registra en la Matriz de Riesgos de Seguridad de la Información, con respecto al activo de información se registran los siguientes datos:

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN			
Proceso	Referencia	Activo de Información	Tipo de Activo

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Para el diligenciamiento de la anterior matriz se describe cada aspecto:

- **Proceso:** Proceso al cual se encuentra asignado el activo de información.
- **Referencia:** Es el número del ítem del activo de información.
- **Activo de Información:** Es el nombre del activo de información.
- **Tipo de Activo:** Corresponde a una de las siguientes categorías:
 - a. Información
 - b. Software
 - c. Hardware
 - d. Servicios
 - e. Intangibles
 - f. Infraestructura crítica cibernética nacional
 - g. Recursos humanos
 - h. Instalaciones y Otros Servicios

4.9.2. Identificación de áreas de impacto

El área de impacto es la consecuencia negativa en los objetivos de la organización en caso de materializarse un riesgo o las que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.

4.9.3. Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la siguiente tabla se definen los elementos necesarios:

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	
Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raíz)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022). Pueden ser **deliberadas (D)**, **fortuitas (F)** o **ambientales (A)**

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Pérdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D

Tipo	Amenaza	Origen
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso

Tipo	Vulnerabilidades
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

4.9.4. Descripción del riesgo

En este paso se identifican:

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		
Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Tipo de Riesgo: Este campo solo admite uno de estos 3 valores:

- Pérdida de Disponibilidad
- Pérdida de Integridad
- Pérdida de Confidencialidad

Descripción del Riesgo: En este campo se describe la situación específica que da como resultado el correspondiente riesgo.

Importante: Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Clasificación del Riesgo: Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.

Paso 2: Análisis de Riesgo Inherente

A partir de este paso metodológico se incorporan la tablas y matrices que desarrollan los lineamientos para los riesgos generales de la gestión.

4.9.5. Determinar la probabilidad

En esta actividad se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		
Frecuencia	% Probabilidad inherente	Probabilidad inherente

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Frecuencia: Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.

% Probabilidad Inherente: Este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa.

Probabilidad inherente: Este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa.

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

4.9.6. Determinar el impacto

En esta actividad se debe realizar el análisis del impacto de la materialización de estos riesgos.

IMPACTO	
% Impacto Inherente	Impacto Inherente

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

% Impacto Inherente: Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa.

Impacto Inherente: Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa.

Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 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

4.9.7. Análisis de severidad

Zona de riesgo inherente: En este campo se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto.

		Impacto				
Probabilidad	Muy Alto 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 20%	Bajo	Bajo	Moderado	Alto	Extremo
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Paso 3: Diseño y Análisis de Controles

4.9.8. Estructura para la Descripción del Control

En esta actividad se seleccionan los controles que se establecerán para mitigar los riesgos.

No. Control	Control Anexo A	Descripción del Control
-------------	-----------------	-------------------------

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

No. Control: Este campo es un consecutivo de los controles a establecer.

Control Anexo A: Este campo corresponde al control seleccionado del Anexo A de la norma 27001:2022.

Nota: Las entidades pueden crear controles adicionales a los listados en el anexo A de la norma ISO 27001:2022 de acuerdo a sus necesidades.

Descripción del Control: Este campo corresponde a una descripción de la forma en la cual el control seleccionado será implementado en la entidad.

Nota: Se recomienda que la entidad establezca para cada control técnico el correspondiente control administrativo, de tal manera que estos se complementen y potencialicen.

4.9.9. Valoración de Controles

Afectación.

En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo.

AFECTACIÓN	
Probabilidad	Impacto

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Probabilidad: En este campo se especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.

Impacto: En este campo se especifica si el control pretende modificar el impacto de ocurrencia de riesgo.

Atributos

En esta actividad se establecen los Atributos de la implementación del control, donde se consideran atributos de eficiencia y los de formalización del control.

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

ATRIBUTOS							
Tipo	%	Implementación	%	Calificación del control	Documentación	Frecuencia	Evidencia

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Paso 4: Valoración de Riesgo Residual

En esta etapa se revisa la efectividad de los controles.

Aplicación de controles para establecer el riesgo residual.

VALORACIÓN DEL RIESGO RESIDUAL				
Probabilidad Residual	% de Probabilidad Residual	Impacto Residual	% Impacto Residual	Zona de Riesgo Final

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Plan de implementación de controles

En esta actividad se establece un plan para implementar los controles y poder realizar el correspondiente seguimiento:

PLAN DE IMPLEMENTACIÓN DE CONTROLES					
Tratamiento	Plan de Acción	Responsable	Fecha de Implementación	Seguimiento	Estado

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

Tratamiento: En este campo se especifica el tipo de tratamiento que se realizará entre 4 opciones disponibles:

- Reducir: Implementar controles para reducir la probabilidad o el impacto
- Compartir: Compartir las consecuencias de la materialización del riesgo, por ejemplo, a través de la adquisición de una ciberpoliza
- Aceptar: Cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección.
- Evitar: Cuando se decide eliminar el activo que es fuente del riesgo: por ejemplo, dar de baja un servidor.

Plan de Acción: En este campo se especifica la identificación del Plan de acción con el cual se realizará la implementación de dicho control.

Responsable: En este campo se especifica el cargo de quien implementa el control.

Fecha de Implementación: En este campo se especifica la Fecha máxima de implementación del control.

Seguimiento: En este campo se especifica la periodicidad del seguimiento a la implementación del control.

Estado: En este campo se especifica el estado de la implementación del control.

Nota: Como parte de la caja de herramientas se encuentra la MATRIZ RIESGOS DE SEGURIDAD DE LA INFORMACIÓN que despliega un ejemplo, como referencia para los análisis requeridos.

4.10. Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP

Teniendo en cuenta la expedición de la Ley 2195 de 2022, que hace obligatorio para las entidades públicas la “prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional” (artículo 31), la Secretaría de Transparencia de la Presidencia de la República sugiere a las entidades obligadas a implementar un Programa de Transparencia y Ética Pública contar con un sistema de gestión que le permita prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral. Para eso, ha diseñado el Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP, que se desarrolla a continuación.

Resaltamos que, en todo caso, atendiendo a lo dispuesto en el parágrafo 1 del artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en aquellas entidades en las que se tenga implementado un Sistema Integral de Administración de Riesgos, este deberá articularse con el Programa de Transparencia y Ética Pública y, en consecuencia, con el Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP.

4.10.1. Integridad pública

Las organizaciones se exponen frecuentemente a que sus objetivos no se cumplan como consecuencia de los diferentes intereses que pueden confluir en la toma de decisiones, en la medida que se privilegian intereses propios sobre el interés general de la organización. En el caso del sector público, el interés general, que no es otra cosa que el interés por la consecución de los fines del Estado, también se puede ver afectado por intereses particulares, lo que termina afectando la capacidad de las entidades públicas para cumplir con las funciones que se le han encomendado.

En este contexto, es donde toma especial relevancia el concepto de integridad en el sector público. Hablar de integridad implica, también, hablar de conceptos como la moral y la ética. La moral hace parte del ámbito personalísimo del individuo, en consecuencia, no es posible

determinarla; por el contrario, la ética presume la capacidad de las personas de comportarse conforme a una serie de expectativas sociales. La integridad, por otro lado, parte de la posibilidad de que una persona, actuando desde un comportamiento ético, se adecue a una serie de códigos de conducta preestablecidos. En esa medida, reconociendo la enorme diversidad de visiones éticas que puede haber en una organización, es posible promover una cultura de integridad entre los colaboradores.

En materia de integridad en el sector público, se espera que los servidores, y en general los colaboradores de las entidades públicas, dentro de un marco ético, se comporten de forma que privilegien el interés general del Estado en todas las decisiones que deben tomar en el ejercicio de sus funciones o del servicio que prestan. Los servidores tienen diferentes normas que establecen ese comportamiento deseado y una máxima en materia de responsabilidad, son responsables tanto de sus acciones como de sus omisiones, tal como lo establece la Constitución Política Colombiana. Así pues, cualquier decisión que no privilegie ese interés es un incumplimiento de la conducta deseable que constituye una actuación que pone en riesgo a la integridad.

En suma, las entidades públicas deben asegurar que exista una cultura de cumplimiento institucional, partiendo del reconocimiento del individuo y su propia ética, para asegurar que éste actúe de forma íntegra, que no es otra cosa distinta que actuar con apego a la ley. Sin embargo, además de una cultura de cumplimiento que promocióne la legalidad, para así garantizar la integridad, es necesario que se adopten medidas para gestionar todas las incertidumbres que pueden poner en riesgo la garantía del interés general, tales como las que se proponen en el capítulo a continuación.

4.10.2. Amenazas para la integridad pública

La Organización para la Cooperación y el Desarrollo Económico, ODCE, ha planteado la necesidad de aplicar un enfoque basado en riesgos cuando se habla de integridad pública⁸. Hay varias amenazas que pueden incidir en diferentes puntos de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en particular, asegurar el cumplimiento de la ley. Para el propósito de esta guía, nos centraremos en cinco amenazas para la integridad, que constituyen una lista enunciativa, en la medida que una entidad pública podría identificar adicionales:

4.10.2.1. Soborno

El Soborno puede ser entendido como “ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como

incentivo o recompensa para que una persona actúe o se abstenga de actuar [...]”⁹. Y opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

El Código Penal Colombiano tipifica el cohecho propio, el cohecho impropio, el cohecho por dar u ofrecer, todos estos delitos contra la administración pública, que son formas de soborno. Solamente entre particulares tipifica de forma general el soborno.

4.10.2.2. Fraude

El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros¹⁰. Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima.

El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

4.10.2.3. Inadecuada gestión del conflicto de intereses

Un conflicto de intereses surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.

Si bien la sola existencia del conflicto de intereses no implica una conducta reprochable, sí existen una serie de comportamientos definidos por códigos de conducta sobre la declaración y gestión del conflicto de intereses. La legislación nacional estima que quien tenga un interés particular en un asunto público está impedido para tomar la decisión.

4.10.2.4. Corrupción

La Corrupción es “todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474

de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral”.

4.10.2.5. Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

4.10.3. Sistema de Gestión del Riesgo

Teniendo en cuenta las diferentes amenazas para la integridad pública, que pueden generar peligro o daño, es necesario que, desde un enfoque basado en riesgos, se gestionen los eventos que pueden ocurrir dentro de una organización. La gestión implica que las entidades deben identificar, analizar y valorar los riesgos, partiendo de la existencia de eventos que pueden convertirse en factores de riesgo.

En este sentido, es necesario que las entidades cuenten con un sistema en el que se interrelacionen e interactúen diferentes elementos para asegurar una gestión integral del riesgo. En esa medida, las entidades deberán contar con un Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP.

El SIGRIP busca articular la Política para la Gestión Integral de Riesgos que formule cada entidad, mediante la cual se gestionan los Riesgos Generales de la Gestión, la Gestión Preventiva de Riesgos Fiscales y los Riesgos de Seguridad de la Información, con los demás elementos que son necesarios para gestionar los riesgos para la integridad pública, que se describen a continuación. Al final, un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causa el soborno, el fraude, un conflicto de intereses gestionado inadecuadamente o la corrupción. Además, puede también favorecer el lavado de activos, la financiación del terrorismo o la financiación de la proliferación de

armas de destrucción masiva. Por esta razón, es necesario abordar los riesgos para la integridad pública de forma integral y en estrecha articulación con la gestión institucional del riesgo.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP contempla que la entidad adopte una serie de instrumentos de gestión del riesgo, que actúe con diligencia en el conocimiento de sus contrapartes y que integre en su operación una función de cumplimiento, todo esto además de la identificación y valoración de los riesgos según la metodología definida en la Política para la Gestión Integral de Riesgos que adopte. Todos estos elementos interactúan para asegurar que la gestión pública se realice de forma íntegra, es decir, con el pleno cumplimiento de la ley en toda la gestión institucional.

El SIGRIP, además, permite a las entidades dar cumplimiento a los lineamientos establecidos para la gestión de riesgos en los Programas de Transparencia y Ética Pública, según lo dispuesto por la Secretaría de Transparencia de la Presidencia de la República. En la medida que se implemente plenamente el Sistema, la entidad estará acreditando la gestión de riesgos para la integridad pública, de riesgos LA/FT/FP, canales de denuncia y debida diligencia.

4.10.3.1. Contexto de la organización

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán realizar un análisis del contexto interno y externo. Para efectos del SIGRIP, ese contexto debe complementarse con los siguientes análisis:

- a. La planta y estructura de la entidad, así como la delegación de autoridad o poder decisorio discrecional dentro de la organización. Para estos efectos, podrá remitirse al mapa de redes internas, al modelo de gobernanza o a la matriz de atribuciones y decisiones, que haya desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.
- b. Los grupos de valor o partes interesadas, incluidos los clientes internos y externos. Se debe hacer especial énfasis en identificar aquellos que pueden considerarse contrapartes, es decir, partes con las que se tienen interacciones, entendidas estas como cualquier tipo de vinculación que involucre la prestación o entrega de un producto, o el intercambio de recursos.
- c. Si la entidad está desconcentrada en el país, identificar los lugares en qué opera. Así mismo, si por su misión, opera en otras jurisdicciones o en sectores, industrias o mercados específicos, identificarlos.

- d. La naturaleza, escala y complejidad de los procesos, servicios, trámites u otras operaciones administrativas de la organización. Dentro de este análisis deben incluirse e identificarse todas las interacciones, es decir, las operaciones con contrapartes que involucran la prestación o entrega de un producto, o el intercambio de recursos.
- e. Información general sobre los contratos y principales proveedores de la entidad. Este análisis implica agrupar a los contratos y proveedores según características como: naturaleza jurídica, modalidad de selección más recurrente, valores mínimos, máximos y media de contratación, relación de cumplimiento o incumplimientos, tipos de supervisión, entre otras variables que pueda construir la entidad para conocer a sus proveedores.
- f. Las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización. Para estos efectos podrá remitirse al mapa de redes externas o al modelo de relacionamiento, que haya desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.
- g. La naturaleza y alcance de las interacciones con entidades de otras Ramas del Poder Público, órganos de control o independientes. Así como de las interacciones con particulares que no derivan en un vínculo formal, pero que son recurrentes (actividades de cabildeo). Para estos efectos podrá remitirse al mapa de redes externas o al modelo de relacionamiento, que haya desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.
- h. Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales. Agrupando entre aquellas que son deberes (obligatorio cumplimiento), expectativas (cumplimiento facultativo) y compromisos (cumplimiento asumido). Para esto podrá remitirse al Marco Normativo que tenga disponible según lo establecido en materia de Transparencia y Acceso a la Información Pública.

4.10.3.2. Liderazgo del Sistema

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán asignar unos niveles de responsabilidad. Además, cuando se habla de la institucionalidad que se requiere para una gestión del riesgo, se menciona como esta actividad involucra a toda la organización y lo relaciona con las diferentes líneas de aseguramiento que actúan en desarrollo del Modelo Estándar de Control Interno. Para efectos del SIGRIP, existen unos roles y responsabilidades que deben agregarse a esos niveles de responsabilidad. Se relacionan en función del esquema de líneas y los roles que existen en los Programas de Transparencia y Ética Pública, los cuales se resumen a continuación:

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	Auditor del Programa	Administrador del Programa	Ejecutores del Programa
Alta Dirección	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Dependencia o persona designada por la Alta Dirección	Directivos, líderes de proceso, servidores y colaboradores
Comité Institucional de Gestión y Desempeño			
Comité Institucional de Coordinación de Control Interno			
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento.	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

4.10.3.3. Planificación

Según lo establecido en esta Guía, las entidades en el marco de la formulación de la Política para la Gestión Integral de Riesgos deberán definir un objetivo y un alcance, así como establecer marco de apetito del riesgo y el esquema metodológico que aplicarán, para lo cual deberán contemplar los siguientes aspectos relevantes del SIGRIP:

- Se debe asegurar que dentro del objetivo se contemple la protección de la integridad pública, teniendo en cuenta que la gestión institucional de riesgos debe estar encaminada a asegurar que la entidad opere en pleno cumplimiento de los códigos que se han establecido, gestionando las diferentes amenazas para el relacionamiento íntegro con el Estado.
- El alcance de la Política debe contemplar los aspectos relevantes de la organización que se hayan identificado del análisis del contexto interno y externo, tales como: los diferentes grupos de valor con los que la entidad se relaciona, particularmente sus contrapartes; las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización; los procesos, servicios, trámites u otras operaciones administrativas de la organización, especialmente aquellas que implican alguna interacción; las jurisdicciones o territorios donde se opera.
- Para el diseño del esquema metodológico, tener en cuenta los lineamientos desplegados a detalle en este documento.

4.10.3.4. Apoyo

Para que el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP pueda operar adecuadamente, la entidad debe disponer de los recursos necesarios, señalar claramente los atributos comportamentales que se requieren, disponer de una estrategia de formación y de comunicación, y documentar cada una de las actividades que se ejecuten; para lo cual:

- La entidad debe identificar los recursos financieros y humanos, soluciones de TI, habilidades especializadas, infraestructura organizacional, material de referencia y experiencia que dispone. Todos estos recursos deben estar claramente identificados en la Política para la Gestión Integral de Riesgos y en cada uno de los elementos del SIGRIP. También, es una oportunidad para identificar el desarrollo y formación profesional que podría requerir para mejorar el Sistema.
- Establecer en la Política para la Gestión Integral de Riesgos las características que debe cumplir las personas que realicen un trabajo que afecte el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, su desempeño y operaciones. En particular, asegurarse que las personas a cargo de la Administración del Programa de Transparencia, que también ejercerían la administración del SIGRIP, sean competentes, es decir, estableciendo requisitos de educación, formación y experiencia apropiados.
- La entidad debe asegurar la toma de conciencia del personal, los líderes, el administrador, la Alta Dirección y, en general, de toda la organización, sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP. En esa medida, debe incluir dentro de la acción de Formación del Programa de Transparencia y Ética Pública la toma de conciencia sobre:
 - a. Los objetivos y alcance del Sistema;
 - b. Cada uno de sus elementos;
 - c. Los beneficios que tiene el Sistema para la organización
 - d. Las implicaciones del incumplimiento de los requisitos del Sistema
- La toma de conciencia sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, también implica comunicar interna y externamente los resultados de su operación, así como cualquier actualización del Sistema o de algunos de sus elementos. Para este propósito, debe incluirse dentro de la acción de Comunicación del Programa de Transparencia y Ética Pública, lineamientos sobre la forma en que se comunicará, periódicamente, los resultados del Sistema, así como cualquier actualización que se introduzca.
- Cada uno de los elementos del Sistema debe estar correctamente documentado. En consecuencia, una vez se implemente, deben llevarse a cabo las gestiones necesarias para incluir en el Sistema de Gestión los documentos del Sistema de Gestión de Riesgos

para la Integridad Pública – SIGRIP, así como en la gestión archivística de la entidad. Para este propósito, la entidad podrá crear y actualizar la información documentada, deberá controlar su gestión, asegurar la protección de los datos personales y la confidencialidad, en el caso de la información clasificada o reservada. En cada elemento del sistema, deberá evaluarse individualmente el tratamiento que debe darse a la información documentada.

4.10.3.5. Operación

Como se indicó previamente, el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP es un conjunto de elementos que operan e interactúan entre sí. El principal elemento del Sistema es la Política para la Gestión Integral de Riesgos, que cada entidad debe formular, junto con su respectivo mapa de riesgos. Esta política define los mecanismos mediante los cuales se identificarán y valorarán los diferentes riesgos a los que está expuesta la organización, incluidos los riesgos para la integridad pública. Sin embargo, esta Política no es suficiente para gestionar completamente los riesgos asociados a soborno, fraude, inadecuada gestión del conflicto de intereses, Corrupción, LA/FT/FP. Entonces, con el propósito de lograr una gestión integral, es que surgen los otros tres elementos del SIGRIP: la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas de gestión del riesgo. La estructura del SIGRIP se observa a continuación.



Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

De acuerdo con la anterior estructura, se procede a describir las particularidades propias del SIGRIP que deben incluirse en la Política para la Gestión Integral de Riesgos, así como cada uno de los elementos adicionales con que debe contar cada entidad, y que en su conjunto derivan en un sistema integral de gestión del riesgo.

4.10.3.5.1. Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos

En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, las entidades deberán identificar y valorar los riesgos que pueden impactar el ejercicio íntegro de la función pública, incluidos los riesgos de LA/FT/FP. La Corrupción es la principal amenaza para la integridad, sin embargo, hay manifestaciones muy específicas de esta práctica que requieren ser identificadas y valoradas individualmente, como lo es el soborno, el fraude y la inadecuada gestión del conflicto de intereses. También, los riesgos por conductas que permiten o favorecen el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, deben ser gestionados, en la medida que la integridad del Estado se ve comprometida cuando sus instituciones se usan para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas.

Sin embargo, bajo una perspectiva de integralidad, los riesgos para la integridad pública deben ser gestionados en conjunto con los riesgos generales de gestión, la gestión preventiva del riesgo fiscal y los riesgos de seguridad de la información. En consecuencia, las entidades deberán contar con una misma Política para gestionar todos sus riesgos.

La existencia de una misma Política para gestionar todos los riesgos implica que se debe aplicar, de forma general, una misma metodología. Es decir, para identificar y valorar los riesgos para la integridad pública se podrá aplicar la propuesta metodológica que se ha definido en este documento. Lo anterior, sin perjuicio de que la metodología pueda ser complementada u objeto de desarrollo por parte de la entidad. Esta Política constituye el estándar mínimo que se debe cumplir, pero cualquier ajuste que se incorpore a la metodología, siempre y cuando sea compatible y no desmejore las condiciones aquí establecidas, es parte de la discrecionalidad que deriva de la autonomía institucional que tienen las entidades públicas.

Así pues, la entidad deberá formular una única Política para la Gestión Integral de Riesgos, que se entenderá parte integral del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, en la que deberá tener en cuenta, respecto de los riesgos para la integridad pública, las siguientes particularidades:

Paso 1: Identificación y descripción del riesgo

1. Respetto de la “Identificación de los puntos de riesgo

En el marco de la gestión del riesgo de LA/FT/FP, debe tenerse en cuenta que los puntos de riesgo se refieren a operaciones que lleva a cabo la entidad. Es decir, actividades dentro del flujo de los procesos que implican un intercambio de recursos, bien sea porque la entidad recibe un bien o servicio por el cual paga un precio, o porque entrega un bien o servicio por el cual le pagan un precio. Estas operaciones son los puntos de riesgo relevantes, que deben tenerse en cuenta para la identificación del riesgo de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

Respetto del riesgo de Corrupción y sus manifestaciones específicas como soborno, fraude e inadecuada gestión del conflicto de intereses, los puntos de riesgos pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones.

2. Respetto de la “Identificación de áreas de impacto”

En el marco de la gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

La consecuencia legal corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños. Así pues, el impacto legal surge desde el momento en que una contraparte es vinculada a procesos judiciales o administrativos sancionatorios o que busquen declarar un incumplimiento.

El contagio corresponde a la posibilidad de que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una entidad o de un individuo relacionado. El contagio se expresa cuando a partes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad.

Las consecuencias legales y de contagio, para efectos de determinar el impacto del riesgo, deben analizarse en términos de afectación económica, atendiendo a lo indicado para cálculo del impacto con las adaptaciones que realice la entidad.

Se puede estimar que un riesgo se ha materializado cuando la situación que se había identificado como posible (riesgo) ocurre realmente y genera un impacto negativo sobre los objetivos. En el caso de los riesgos para la integridad pública, el riesgo se materializa siempre que se advierta un impacto sobre la reputación, la operación o de cumplimiento o que comprometa la ejecución del recurso.

La consecuencia reputacional, por ejemplo, surge cuando la organización se ve involucrada en denuncias o reportajes que la vinculan con prácticas poco íntegras, incumplimientos normativos o corrupción en general. La consecuencia operativa corresponde a los escenarios en que la conducta contraria a la integridad termina afectando el desarrollo de los procesos. La consecuencia legal inicia desde el mismo momento en que una parte vinculada es involucrada en procesos que puedan derivar en una sanción y el contagio se da cuando la involucrada es la parte relacionada. Finalmente, la consecuencia económica puede configurarse, incluso, desde el mismo momento en que hay retrasos en la ejecución del recurso, por conductas poco íntegras del ejecutor.

En la medida que la gestión del riesgo de LA/FT/FP está centrada en prevenir la utilización de la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas, aun cuando no haya consecuencias, toda operación sospechosa, incluso la intentada, debe ser objeto de reporte, al margen de la materialización del delito de lavado de activos.

La materialización del riesgo no debe confundirse con la ocurrencia del delito, falta o conducta generadora de responsabilidad fiscal. Es posible que el riesgo se haya materializado, es decir, que haya un impacto con consecuencias negativas para la entidad, incluso antes de la vinculación formal a procesos sancionatorios. También, es posible que el riesgo se materialice aun cuando la persona termine absuelta. Por lo anterior, los riesgos para la integridad no deben entenderse como tipos penales o disciplinarios, ni la materialización del riesgo implica un prejuizgamiento.

Toda la gestión del riesgo tiene como principales objetivos la identificación, medición, control y el monitoreo, con el propósito de prevenir, detectar y corregir. En ningún caso podrá derivar en juicios de responsabilidad o en la aplicación de sanciones. Ante un escenario de materialización de un riesgo, la respuesta institucional debe estar encaminada a asegurar la “continuidad del negocio”, es decir, a asegurar que, a pesar del impacto que hubo en los objetivos derivados del riesgo que se materializa, estos se puedan cumplir. En esa medida, la Política para la Gestión Integral de Riesgos debe propender por asegurar continuidad del servicio y/o la operación normal de la organización en todos los escenarios de materialización de riesgos para la integridad, con independencia de las actuaciones que, por competencia, correspondan a otras autoridades, incluso antes de que existan decisiones de fondo que resuelvan los temas de responsabilidad.

3. Respetto de la “Identificación de factores de riesgo”

Como factores del riesgo LA/FT/FP se tiene a las contrapartes, los productos, los canales y las jurisdicciones, aspectos mínimos a contemplar en cualquier análisis, los cuales en

conjunto conforman el concepto de “transacción” u “operación”, en el entendido que una transacción, en todos los casos, será realizada por un cliente o usuario, que accedió o entregó un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica. Estos factores deben permitirle a la entidad mayor efectividad en el conocimiento de las contrapartes, el diseño y aplicación de señales de alerta, la identificación de operaciones inusuales y la determinación y el reporte de operaciones sospechosas.

Surge, entonces, la necesidad de segmentación de los factores de riesgo, a partir de la cual, se profundiza tanto en el conocimiento de las contrapartes, así como de los factores de riesgo con los que tienen relación.

El objetivo y los beneficios de la segmentación de los factores de riesgo se encuentran en la identificación de grupos con características y comportamientos similares, en los que se garantiza la homogeneidad al interior de los segmentos y la heterogeneidad entre los mismos, de acuerdo con el análisis técnico de variables de información.

Al garantizar las características de homogeneidad y heterogeneidad, cada uno de los segmentos genera implícitamente los parámetros normales de comportamiento transaccional de los miembros de cada grupo, lo que se entiende como los límites de operación de cada persona o comúnmente denominadas como las señales de alerta que se encargan de la identificación de las operaciones que salen de la normalidad identificada y que pueden ser catalogadas como operaciones inusuales objeto de estudio por parte de la función de cumplimiento, con el fin de efectuar los reportes oportunos a las autoridades competentes.

En este sentido, las entidades deben incorporar en la Política para la Gestión Integral de Riesgos, la obligación de mantener los documentos y registros de las contrapartes y sus operaciones por el término dispuesto en el artículo 12 de la Ley 2195 de 2022; y asignar los recursos técnicos, tecnológicos y de talento humano para poder llevar a cabo la gestión de estos riesgos. La Política, además, debe describir la segmentación de los factores de riesgo LA/FT/FP, que derivan del análisis de contexto realizado. Para efectos de la metodología que permita construir las señales de alerta, pueden referirse al capítulo sobre indicadores clave de riesgo.

4. Respecto de la “Descripción del riesgo”

La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en este documento. Todos iniciarán con la fórmula “Posibilidad de”, y deben señalar el impacto, la causa inmediata y la causa raíz.

Teniendo en cuenta las amenazas descritas, las causas inmediatas de los riesgos para la integridad pública podrán ser el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.

De acuerdo con lo anterior, se sugiere tener en cuenta los siguientes ejemplos desplegados a continuación:

Impacto	Causa inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar [...].	
	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar [...].	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un 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, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

En ese orden de ideas, para cada riesgo y su causa inmediata, atendiendo la estructura para la redacción del riesgo definida en el numeral 3.4 se tendría lo siguiente:

- Posibilidad de afectación económica por Corrupción en la evaluación en la evaluación de los procesos de selección para la contratación de bienes y servicios de la Entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico.
- Posibilidad de afectación económica por Fraude Interno en la asignación de subsidios a causa de errores, omisiones, informes inexactos o descripciones incorrectas realizados para beneficio personal o de terceros en la asignación de subsidios.
- Posibilidad de afectación reputacional por Soborno Saliente en el seguimiento a la agenda legislativa de la Entidad, a causa del ofrecimiento indebido de incentivos o

recompensas para que una persona actúe o se abstenga de actuar en favor de la entidad.

- Posibilidad de afectación reputacional por Soborno Entrante al aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.
- Posibilidad de afectación económica por conflicto de interés no declarado y/o declarado, pero no gestionado y/o declarado y no aceptado, a causa de decisiones en asuntos sobre los cuales la servidora o servidor público tiene un interés particular en desarrollo del comité de contratación.

En el caso particular del riesgo LA/FT/FP, debe hacerse referencia particularmente a las actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo.

Impacto	Causa Inmediata	Causa Raíz
Económico, Reputacional, Legal, Operativo o de Contagio	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva	Descripción de la Operación o Transacción

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas en las operaciones de pago de subsidios.

- Posibilidad de contagio por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de contratación directa.
- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de recaudo.

Paso 2: Análisis de Riesgo Inherente

5. Respecto del “Análisis de Riesgo Inherente”

Por la naturaleza de los riesgos para la integridad pública, el objetivo fundamental es prevenirlos, detectarlos y reportarlos en términos de oportunidad y eficacia. Esta perspectiva debe ser transversal al análisis del riesgo y al diseño de controles.

Para el cálculo de probabilidad e impacto, aplica lo establecido en el presente documento y los ajustes que la entidad considere incorporar en los descriptores, atendiendo su naturaleza, recursos, estructura para la operación y capacidades específicas. Así mismo, aplica la matriz de severidad ya definida, la cual no es susceptible de ajustes.

Paso 3: Diseño y Análisis de Controles

6. Respecto del “Diseño y análisis de controles”

Para el diseño de controles deberá tenerse en cuenta que, además de la Política para la Gestión Integral de Riesgos y su respectivo Mapa de Riesgos, las entidades deberán desarrollar, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, un Manual para el desarrollo del principio de debida diligencia, contar con una función de cumplimiento y formular una serie de herramientas de gestión. Al final, estos elementos adicionales del Sistema son el repertorio de controles que tiene la entidad y que pueda aplicar en cada uno de los riesgos identificados, sin perjuicio de que puedan desarrollarse controles adicionales o muy específicos.

En todo caso, se sugiere que las políticas, procedimiento o códigos que se establezcan como controles se incorporen en la Política para la Gestión Integral de Riesgos o en el Programa de Transparencia y Ética Pública, para asegurar la integralidad del Sistema.

Por lo demás, para el diseño y análisis de controles deberán referirse al que establece la estructura general, los atributos y tablas para su valoración.

Paso 4: Valoración de Riesgo Residual

7. Respecto de la “Valoración del riesgo residual”

Sobre este punto referirse completamente al numeral 4.7.12. de este documento.

4.10.3.5.2. Debida diligencia en el conocimiento de las contrapartes

Las entidades deben contar con lineamientos y procedimientos internos sobre la debida diligencia con que deben llevar a cabo el conocimiento de sus contrapartes. Así lo establece la Ley 2195 de 2022, que dispone:

ARTÍCULO 12. PRINCIPIO DE DEBIDA DILIGENCIA. La Entidad del Estado y la persona natural, persona jurídica o estructura sin personería jurídica o similar, que tenga la obligación de implementar un sistema de prevención, gestión o administración del

riesgo de lavado de activos, financiación del terrorismo y proliferación de armas o que tengan la obligación de entregar información al Registro Único de Beneficiarios Finales (RUB), debe llevar a cabo medidas de debida diligencia que permitan entre otras finalidades identificar el/los beneficiario(s) final(es), teniendo en cuenta como mínimo los siguientes criterios:

1. Identificar la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal.
2. Identificar el/los beneficiario(s) final(es) y la estructura de titularidad y control de la persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal, y tomar medidas razonables para verificar la información reportada.
3. Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico o el contrato estatal. Cuando la entidad estatal sea la contratante debe obtener la información que permita entender el objeto social del contratista.
4. Realizar una debida diligencia de manera continua del negocio jurídico o el contrato estatal, examinando las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones sean consistentes con el conocimiento de la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se realiza el negocio jurídico o el contrato estatal, su actividad comercial, perfil de riesgo y fuente de los fondos.
5. El obligado a cumplir con el principio de debida diligencia del presente artículo, debe mantener actualizada la información suministrada por la otra parte.

De acuerdo con lo anterior, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, cada entidad deberá contar con un Manual que incorpore mecanismos que desarrollen el principio de debida diligencia en todas las interacciones con contrapartes, en las que exista una exposición a riesgos para la integridad pública, es decir, en aquellas interacciones en que se haya identificado un riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

El principio de debida diligencia se materializa en políticas y procedimientos para identificar, analizar y evaluar los riesgos y oportunidades en una interacción, operación o relación con contrapartes, con el objetivo de tomar decisiones informadas. En esa medida, como principio debe aplicarse en concordancia con los principios de razonabilidad y proporcionalidad. Lo razonable se refiere a que todo mecanismo debe ser adecuado para los fines que persigue y necesario para alcanzarlos. Lo proporcional a que los mecanismos se apliquen desde un enfoque basado en riesgos. Así pues, el Manual debe: (1) ser diseñado de tal forma que pueda ser cumplible por la entidad, teniendo en cuenta sus recursos

disponibles [razonabilidad]; (2) contemplar diferentes niveles de complejidad para que se aplique según el nivel de riesgo para la organización.

El conocimiento de las contrapartes consiste en la obtención de información de la contraparte, de las operaciones y de los productos involucrados en la relación que le permitan a la entidad gestionar adecuadamente los riesgos. El resultado de estos mecanismos tiene como único propósito generar insumos para la toma de decisiones, pero no podrá derivar en inhabilidades o incompatibilidades diferentes a las contempladas en la legislación vigente. Sin embargo, en el marco de la gestión del riesgo, la entidad sí podrá atribuir consecuencias a partir del conocimiento que alcance de sus contrapartes, entre ellos:

- La identificación de señales de alerta que deben ser atendidas por la organización.
- La necesidad de implementar controles adicionales, especiales o revisar los existentes para ajustarlos a los resultados de la aplicación del mecanismo de conocimiento de la contraparte.
- La necesidad de hacer ajustes en los equipos a cargo del relacionamiento con la contraparte o que se requieran aprobaciones adicionales, de instancias superiores o plurales, para continuar la relación.
- En circunstancias excepcionales, podrá evaluarse la necesidad de terminar con la relación o abstenerse de iniciarla, en cuyo caso tendrá que aplicarse la normativa especial que aplique.
- Un monitoreo especial a las operaciones que se realicen en el marco del relacionamiento para generar los reportes cuando estas sean inusuales o sospechosas, ante las autoridades correspondientes.

Ahora bien, en la medida que el conocimiento de las contrapartes debe tener un efecto preventivo, los mecanismos deben ser aplicados antes de establecer cualquier relación. Sin embargo, eso no excluye pueda haber un monitoreo permanente y continuo mientras dure el relacionamiento, para detectar cambios que afecten el nivel de riesgo.

La entidad debe garantizar que los resultados de la aplicación de los mecanismos para conocimiento de las contrapartes queden documentados dentro de la organización adecuadamente, para eso debe asegurar la confidencialidad de la información clasificada y reservada, el correcto tratamiento de los datos personales y su archivo y custodia, según la normativa aplicable.

Todo lo anterior debe quedar contemplado en el Manual que elaboró la entidad, el cual debe cumplir con las siguientes características:

1. Establecer lineamientos de debida diligencia:
 - a. Preparación: (1) definir los objetivos de la debida diligencia; (2) determinar los procesos clave en los que se aplicará; (3) identificar dentro de los equipos de trabajo que la llevaran a cabo.
 - b. Recolección de información: (1) determinar las fuentes de información, como estados financieros, contratos, informes legales, listas restrictivas y vinculantes, etc., que se consultaran; (2) determinar la procedencia de entrevistas, inspecciones o visitas a la contraparte.
 - c. Análisis: (1) establecer los criterios para determinar los casos en que hay lugar a un problema, inconsistencia o riesgo; (2) establecer el procedimiento de evaluación de la información obtenida antes de la vinculación o relación; (3) establecer los estándares normales de funcionamiento de la organización, según el análisis de contexto realizado, y del sector, industria o mercado en que se dará la vinculación o relacionamiento, para determinar los patrones normales.
 - d. Informe de resultados: (1) indicar el contenido detallado de los informes que se generaran como resultado de la aplicación de los mecanismos de conocimiento con hallazgos clave y riesgos identificados; (2) el informe debe contener una evaluación sobre la viabilidad de la vinculación o relación con base en los hallazgos; (3) el informe debe incluir recomendaciones para mitigar o gestionar los riesgos encontrados.
2. Establecer un procedimiento y lista de verificación, para la consulta en los siguientes listados:
 - a. Sistema de Información del Boletín de Responsables Fiscales – SIBOR, de la Contraloría General de la República.
 - b. Sistema de Información de Registro de Sanciones e Inhabilidades – SIRI, de la Procuraduría General de la Nación.
 - c. Antecedentes Penales y Requerimientos Judiciales, de la Policía Nacional de Colombia.
 - d. Sistema Registro Nacional de Medidas Correctivas – RNMC, de la Policía Nacional de Colombia.
 - e. Registro de Deudores Alimentarios Morosos – REDAM, del Ministerio de Tecnologías de la Información y las Comunicaciones.
 - f. Lista consolidada del Consejo de Seguridad de las Naciones Unidas, que incluye, pero sin limitarse, las Resoluciones 1267 de 1999, 1988 de 2011, 1373 de 2001, 1718 y 1737 de 2006 y 2178 de 2014 del Consejo de Seguridad de las Naciones Unidas, y todas aquellas que le sucedan, relacionen y complementen, y cualquiera otra lista que se adopte formalmente por el país.
 - g. Lista vigente de terroristas de Estados Unidos de América.
 - h. Lista vigente de la Unión Europea de Organizaciones Terroristas.

- i. Lista vigente de la Unión Europea de Personas Catalogadas como Terroristas.

La consulta deberá hacerse respecto de las contrapartes que sean personas naturales y del representante legal y suplente, revisor fiscal y beneficiarios finales de las contrapartes que sean personas jurídicas u otras estructuras.

3. Establecer un procedimiento para la verificación de la identidad de las contrapartes y evaluación de su historial, lo cual es fundamental para detectar cualquier vinculación con actividades sospechosas. Para lo cual se deberá:

- a. Identificar el nombre o razón social la contraparte.
- b. Determinar la existencia y representación legal. Las personas naturales lo acreditan con su cédula; las personas jurídicas con los certificados expedidos por las cámaras de comercio; otras estructuras con su acto de creación y Registro Único Tributario, si aplica.
- c. En el caso de personas jurídicas u otras estructuras, identificar la estructura de propiedad y existencia de situaciones de control¹⁶.
- d. En el caso de personas jurídicas u otras estructuras, identificar los beneficiarios finales¹⁷.
- e. Evaluar las relaciones que ha tenido la contraparte con entidades similares en un período de dos (2) años anteriores al relacionamiento, siempre y cuando la contraparte tenga dos o más años de existencia. Para estos efectos, la entidad podrá solicitar referencias de, al menos, dos entidades similares con que la contraparte haya estado relacionada.
- f. Determinar si la contraparte cuenta con un Programa de Transparencia y Ética Pública o Empresarial, o con políticas Antilavado de Activos, Antisoborno o Anticorrupción.
- g. Verificar la documentación aportada para acreditar cualquier hecho en el marco de la relación, como formación, experiencia, capacidad financiera y organizacional, etc.
- h. Verificar, por los medios disponibles, la reputación de la contraparte. Para esto, la entidad podrá revisar noticias e información pública que esté disponible en internet y hacer uso de herramientas de inteligencia artificial.
- i. Requerir declaraciones sobre la fuente de los recursos que utilizará en el marco de la relación que mantenga con la entidad, con sus debidos soportes.
- j. Verificar si la contraparte tiene procesos administrativos sancionatorios, disciplinarios, de responsabilidad fiscal, penales o judiciales, que estén activos o en curso ante las autoridades colombianas.

Toda esta información busca asegurar que la entidad entienda claramente el propósito y el carácter que se pretende dar a la interacción o relación establecida. Sin embargo, atendiendo al principio de proporcionalidad, y desde un enfoque basado en riesgos, es posible que no se requiera en todos los casos conocer toda la información. Así pues, en cada Manual las entidades podrán establecer criterios diferenciales para aplicar una debida

diligencia simplificada, cuando la relación tiene un riesgo bajo; una debida diligencia estándar, para riesgo medio; o una debida diligencia ampliada, en los casos de riesgo alto.

El listado de verificación mencionado es enunciativo. En el Manual, la entidad podrá agregar otras verificaciones de identidad de las contrapartes y evaluación de su historial, según lo estime pertinente o su capacidad lo permita.

4. Establecer un lineamiento respecto de los casos en que se identifique que una de las contrapartes es una Persona Expuesta Políticamente, según la definición del artículo 2.1.4.2.3 del Decreto 1081 de 2015. Sobre este punto se debe resaltar que la calidad de Persona Expuesta Políticamente (PEP) se mantendrá en el tiempo durante el ejercicio del cargo y por dos (2) años más desde la dejación, renuncia, despido o declaración de insubsistencia del nombramiento, o de cualquier otra forma de desvinculación, o terminación del contrato. La debida diligencia debe incluir una investigación más profunda sobre estas contrapartes, ya que pueden estar expuestos a mayores riesgos para la integridad pública.

5. Establecer lineamientos para la toma de decisiones basada en los resultados de la debida diligencia:

- a. El Manual debe identificar los procesos en que se deben aplicar los mecanismos de conocimiento de la contraparte. Deben incluirse todos aquellos en que se ha identificado riesgos para la integridad pública. En cada proceso, se deben identificar, además, las operaciones, vinculaciones o relaciones que tienen exposición a riesgos para la integridad pública.
- b. El Manual debe establecer como una política institucional incluir en todos los procesos donde se identifiquen operaciones, vinculaciones o relaciones expuestas a riesgos, la adopción de un punto de control relacionado con la aplicación de mecanismos de conocimiento de las contrapartes.
- c. La política, además, debe indicar cómo se realizará la discusión de los hallazgos, y cómo se tomarán decisiones sobre si proceder, modificar o cancelar la operación, vinculación o relación.

6. Establecer un lineamiento para el tratamiento de los hallazgos y las “posdevida diligencia”

- a. En el Manual la entidad debe incluir una política que establezca el margen de acción posible ante eventuales hallazgos, contemplando los ajustes que puede realizar la entidad en los términos del acuerdo para mitigar riesgos.
- b. Es fundamental resaltar que no en todos los casos la debida diligencia deriva en una inhabilidad, sin embargo, los hallazgos deben ser objeto de tratamiento.

- c. El tratamiento de los hallazgos puede ir desde cambios en los términos del acuerdo; supervisión especial a la operación, vinculación o relacionamiento; la transferencia del riesgo; solicitar garantías adicionales de cumplimiento o requisitos complementarios; el reporte a autoridades; etc. Los posibles tratamientos los define cada entidad y se pueden ir ajustando conforme la experiencia institucional en gestión del riesgo se haga más compleja.
- d. En la política debe quedar contemplada la obligación de la entidad de examinar continuamente, a lo largo de la vinculación o relación, las operaciones llevadas a cabo por la contraparte relacionada con los hallazgos, para asegurar que sean consistentes con el conocimiento que se tiene de la contraparte, su actividad económica y su perfil de riesgo.
- e. Se consideran como alertas que pueden derivar en potenciales hallazgos que requieren tratamiento:
 - No haber identificado plenamente a la contraparte, incluyendo, no conocer sus beneficiarios finales.
 - La existencia de procesos activos o en curso que involucren a la contraparte, haber obtenido referencias negativas o malos antecedentes en la revisión de la reputación. En el caso de las personas jurídicas u otras estructuras, aplicará respecto del representante legal principal y suplente, el revisor fiscal y los miembros de junta directiva, los controlantes y el beneficiario final.
 - Los precios son considerablemente distintos a los normales del mercado, aun cuando no fueron considerados artificiales.
 - La contraparte se financia con recursos internacionales que se originan en países no cooperantes o jurisdicciones de riesgo, según lo defina la normativa nacional.
 - La relación implica que la contraparte deberá contar con subcontratistas.
 - La contraparte está registrada en los listados internacionales vinculantes para el país de personas y entidades asociadas con organizaciones terroristas. En el caso de las personas jurídicas u otras estructuras, aplicará respecto del representante legal principal y suplente, el revisor fiscal y los miembros de junta directiva, los controlantes y el beneficiario final.

7. Establecer un lineamiento para informar a las autoridades de los hallazgos.

Si se detecta alguna actividad intentada o sospechosa de lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva, la entidad está obligada a informar a las autoridades competentes, como la Unidad de Información y Análisis Financiero (UIAF) o Fiscalía General de la Nación. Esto es parte del cumplimiento con las leyes. Dentro de las herramientas de gestión, la entidad debe contemplar un procedimiento para la identificación de estas operaciones sospechosas, por lo que en el Manual solo debe quedar contemplada la política de informar este tipo de hallazgos, así

como cualquier otro que se configure como un potencial delito o falta a las autoridades competentes.

4.10.3.5.3. Función de cumplimiento

La función de cumplimiento implica, entre otros aspectos:

- a. Velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto, y cada uno de sus elementos, promoviendo el cumplimiento de sus disposiciones y apoyando a los líderes de procesos y gestores de riesgo, en la gestión de los riesgos identificados. Para estos efectos, se podrán generar políticas o procedimientos internos, vinculantes para la organización.
- b. Evaluar el SIGRIP y presentar, en la periodicidad que se establezca, los resultados de la evaluación a la Alta Dirección. Las evaluaciones deberán contemplar, además:
 - Los resultados de la gestión desarrollada en el marco de la función de cumplimiento.
 - Los reportes de operaciones generados en el marco de la gestión del riesgo.
 - Los planes de mejoramiento del SIGRIP implementados, en el marco del proceso de mejora continua.
- c. Revisar y recomendar la implementación de los lineamientos que el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República, la Unidad de Información y Análisis Financiero, y las entidades de control, expidan en temas relacionados con la gestión del riesgo.
- d. Promover la adopción de correctivos del SIGRIP y adoptar aquellos que estén dentro de su competencia.
- e. Articular con las dependencias correspondientes las gestiones pertinentes para la operatividad del SIGRIP, así como el desarrollo de programas internos de capacitación en materia de cumplimiento y gestión del riesgo.
- f. Proponer a la Alta Dirección la actualización de los elementos del SIGRIP y velar por su comunicación oportuna a todas las partes interesadas.
- g. Colaborar con el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos que requiera el SIGRIP y aplicarlos según corresponda.
- h. Establecer los lineamientos institucionales para la aplicación proporcional basada en riesgos de los mecanismos de debida diligencia en el conocimiento de las contrapartes.
- i. Elaborar y someter a aprobación de la Alta Dirección, los criterios objetivos para la determinación de las operaciones inusuales y sospechosas.
- j. Reportar a la Unidad de Información y Análisis Financiero, a la Fiscalía General de la Nación o a la autoridad que corresponda, las operaciones intentadas o sospechosas que se hayan identificado conforme a los criterios definidos y el procedimiento institucional adoptado.

No es necesario que las entidades públicas creen cargos específicos para asumir esta función de cumplimiento. Según lo establecido en el Decreto 1083 de 2015, por regla general, cualquier servidor del nivel directivo, o su equivalente según el sistema de empleo público con que cuente la entidad, podría asumirla al estar relacionada con las funciones generales que tiene este tipo de cargo, en particular, la de “adelantar las gestiones necesarias para asegurar el oportuno cumplimiento de los planes, programas y proyectos y adoptar sistemas o canales de información para la ejecución y seguimiento de los planes del sector”. Incluso esta función podría ser asumida por servidores del nivel asesor, que tienen, entre otras funciones, la de “absolver consultas, prestar asistencia técnica, emitir conceptos y aportar elementos de juicio para la toma de decisiones relacionadas con la adopción, la ejecución y el control de los programas propios del organismo”.

Bajo las anteriores premisas, es pertinente indicar que la función de cumplimiento puede ser asignada dentro de las plantas de personal existentes en la mayoría de las entidades públicas. Lo anterior, sin perjuicio de que la entidad decida crear un cargo específico.

En ese orden de ideas, para asignar la función de cumplimiento, deberán tenerse en cuenta los siguientes aspectos:

- a. La función puede ser asignada a una persona, grupo o dependencia, según las capacidades de la entidad. Se recomienda tener en cuenta: la estructura organizacional, la planta y cargas de trabajo, la complejidad de las operaciones y el nivel de exposición a los riesgos para la integridad pública, para determinar la capacidad que debe tener la persona, grupo o dependencia que tendrá la función de cumplimiento.
- b. La función debe estar asignada dentro del segundo nivel jerárquico de la entidad. Es decir, la persona, grupo o dependencia debe responder directa y exclusivamente a la Alta Dirección.
- c. La persona, grupo o dependencia, preferiblemente, debe dedicarse exclusivamente a desarrollar la función de cumplimiento. Sin embargo, en el evento en que la función se asigne a una persona, grupo o dependencia que no tenga dedicación exclusiva y desempeñe funciones adicionales, la Entidad debe contar con mecanismos para prevenir y gestionar los conflictos de intereses que puedan surgir producto del ejercicio de otras funciones que podrían ser objeto de evaluación.
- d. La entidad debe asegurar que la persona, grupo o dependencia se capacite de forma permanente en temas de gestión de riesgos, transparencia, integridad, sistemas de gestión antisoborno, antifraude y de cumplimiento; además deben estar actualizados en los lineamientos de la Política Nacional Antilavado de Activos, contra la Financiación del Terrorismo y contra la Financiación de la Proliferación de Armas de Destrucción Masiva.

- e. A quien se asigne la función de cumplimiento o quienes integren el grupo de trabajo o dependencia, deberán ser personas reconocidas dentro de la organización por su probidad, ética y que cumplan diligentemente con sus obligaciones, en consecuencia: no podrá haber investigaciones de ningún tipo en su contra; los resultados de sus evaluaciones de desempeño deben ser satisfactorios; deberá haber realizado las declaraciones de bienes y rentas, y de conflictos de interés, de forma oportuna y mantenerlas actualizadas según la normativa vigente.
- f. Quien asuma la función de cumplimiento podrá asumir, también, el rol de administrador del Programa de Transparencia y Ética Pública de la entidad.

Una vez la entidad asigne la función de cumplimiento dentro de la organización, debe informar a la Secretaría de Transparencia de la Presidencia de la República el nombre, teléfono de contacto y correo electrónico de la persona quien asuma la función o que lidere el grupo o dependencia. La entidad debe asegurar que la información sobre la identidad y medios de contacto se mantenga actualizada, por lo cual deberá informar a la Secretaría cualquier cambio máximo dentro del mes siguiente a la ocurrencia de la novedad. Este acto es meramente informativo y no condiciona el ejercicio de la función, ni implica que debe tomarse algún tipo de posesión ante la Secretaría de Transparencia.

La función de cumplimiento no sustituye, elimina o restringe las funciones propias de las unidades de control interno.

Excepcionalmente, la entidad podrá contratar a particulares para que apoyen la gestión de cumplimiento. En estos casos, deberán llevar a cabo procesos de selección de conformidad con lo establecido en el Estatuto General de Contratación de la Administración Pública, que deberán atender a las siguientes consideraciones:

- a. Solo podrá acudir a la contratación en aquellos casos que la entidad acredite no contar con el personal suficiente en su planta para poder asignarle la función de cumplimiento. Dada la relevancia especial que tiene esta materia, el certificado de inexistencia de personal debería estar suscrito por el representante legal de la entidad y contener un análisis completo de la estructura y la planta, que permita concluir de forma inequívoca que a ningún servidor del nivel directivo o asesor se le puso asignar dicha función.
- b. Deberán contratarse servicios profesionales especializados, para lo cual, las entidades deberán incluir en los documentos del proceso como requisitos: (1) formación específica en temas relacionados con cumplimiento, gestión del riesgo LA/FT/FP o conexos con el SIGRIP; (2) experiencia específica y relacionada de, mínimo, un (1) año en gestión del riesgo en entidades públicas, gestión del riesgo LA/FT/FP o como oficial de cumplimiento.

- c. Deberá incluirse en los documentos del proceso un requisito que establezca que, al momento de presentación de la oferta, el oferente no puede estar vinculado a más de tres entidades públicas prestando el servicio de apoyo a la gestión de cumplimiento. Así mismo, debe incluirse como requisito una declaración del oferente informando a la entidad si está vinculado a otras entidades públicas prestando el mismo servicio o servicios similares de apoyo a la gestión de cumplimiento.

4.10.3.5.4. Herramientas de gestión del riesgo

Además de contar con una Política para la Gestión Integral de Riesgos, un Mapa de Riesgos, un Manual de Debida Diligencia en el Conocimiento de las Contrapartes y una función de cumplimiento distribuida dentro de la organización, la gestión de riesgos para la integridad pública requiere que la organización implemente una serie de políticas, procedimientos y códigos de conducta, que contribuyen a la integralidad del sistema.

- a. Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP). La entidad deberá formular una política institucional que, expresamente: manifieste el compromiso de la Alta Dirección con una cultura de prevención y mitigación del LA/FT/FP; prohíba y rechace cualquier practica asociada al LA/FT/FP; obligue a la entidad a cumplir con la normativa ALA/CFT/CFP; obligue a actuar con debida diligencia en el conocimiento de las contrapartes; promocióne la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias; informe las consecuencias del incumplimiento de la política.
- b. Política Antisoborno. La entidad deberá formular una política institucional que, expresamente: manifieste el compromiso de la Alta Dirección con una cultura de prevención y mitigación del soborno; tipifique las prácticas de soborno; prohíba y rechace cualquier practica asociada al soborno; obligue a la entidad a cumplir con la normativa antisoborno; obligue a actuar con debida diligencia en el conocimiento de las contrapartes; promocióne la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias; informe las consecuencias del incumplimiento de la política.
- c. Política Antifraude. La entidad deberá formular una política institucional que, expresamente: manifieste el compromiso de la Alta Dirección con una cultura de prevención y mitigación del fraude; tipifique las prácticas de fraude; prohíba y rechace cualquier practica asociada al fraude; obligue a la entidad a cumplir con la normativa antifraude; promocióne la denuncia de cualquier actividad que esté asociada a las señales de alerta definidas por la entidad, sin temor a represalias; informe las consecuencias del incumplimiento de la política.

- d. Procedimiento para la gestión de los conflictos de intereses. La entidad deberá formular un procedimiento interno que, expresamente: contenga un catálogo de situaciones que se podrían presentar dentro de la organización, con ejemplos reales, que generen un conflicto de intereses; el paso a paso que debe seguir cualquier persona para declarar un conflicto de intereses al interior de la organización; el paso a paso que seguirá la entidad para tramitar un conflicto de intereses; el margen de acción de la entidad para gestionar los conflictos de intereses; el paso a paso para realizar las declaraciones periódicas que la ley establezca; el paso a paso para controlar que se hayan realizado las declaraciones periódicas que la ley establece.
- e. Procedimiento para el reporte de operaciones sospechosas. La entidad deberá formular un procedimiento interno que, expresamente: establezca los criterios y señales de alerta para determinar que una operación es inusual; el paso a paso para que los líderes de proceso reporten a quien ostente la función de cumplimiento las operaciones inusuales; el paso a paso para que quien ostenta la función de cumplimiento evalúe la operación inusual y determine si es sospechosa; el paso a paso para reportar a las autoridades competentes la operación sospechosa, incluso cuando fue intentada.
- f. Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético. La entidad deberá formular un procedimiento interno que, expresamente: identifique los medios de recepción de denuncias e inquietudes; el paso a paso para evaluar las denuncias e inquietudes que se presenten por el canal; el paso a paso para tratar las denuncias e inquietudes que correspondan al canal; el paso a paso para concluir el trámite de las denuncias e inquietudes, de conformidad con el tratamiento realizado.

Todas las herramientas de gestión deben desarrollarse en los Programas de Transparencia y Ética Pública de las entidades. La Política para la Gestión Integral de Riesgos, el Mapa de Riesgos, y el Manual de Debida Diligencia en el Conocimiento de las Contrapartes, también, hacen parte integral del Programa de Transparencia.

La Secretaría de Transparencia de la Presidencia de la República pondrá a disposición de las entidades herramientas modelo, que podrán ser adoptadas de forma voluntaria. Lo anterior, sin perjuicio de que, también de manera voluntaria, las entidades decidan implementar sistemas estandarizados en aquellas herramientas de gestión que cuentan con guías o normas técnicas aprobadas por organismos de normalización.

4.10.3.6. Monitoreo, evaluación, auditoría y mejora

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto permanente de monitoreo, evaluación, auditoría y mejora. Para este propósito, deben tenerse en cuenta las siguientes consideraciones:

- a. En la Política para la Gestión Integral de Riesgos debe quedar establecido la periodicidad y el contenido del monitoreo a los riesgos que gestiona el SIGRIP. El monitoreo, que consiste en el seguimiento que se hace para determinar el estado del Sistema, corresponde a la primera línea de defensa, particularmente, a los líderes de proceso. En esa medida, los líderes, junto con sus equipos, son los responsables de generar los reportes que la organización determine sobre el estado de la gestión de riesgos en el marco del SIGRIP, y remitirlos al Administrador.
- b. Corresponde al Administrador del Programa, desde su rol como segunda línea de defensa, la evaluación de la gestión del riesgo. La evaluación implica determinar el cumplimiento de los objetivos definidos para el Sistema y de cada uno de sus elementos. Para esto, corresponde al Administrador medir y analizar los resultados del monitoreo, de forma que pueda llevar a cabo una evaluación objetiva. Para este propósito deben tenerse en cuenta los indicadores asociados a la gestión del riesgo que se definan y establecer los reportes que se requieren de la primera línea. En la Política para la Gestión Integral de Riesgos deben definirse la periodicidad y los contenidos de la evaluación al SIGRIP.
- c. El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto de auditoría, la cual estará a cargo de la unidad de control interno o quien ejerza la tercera línea de defensa. La auditoría debe realizar una evaluación independiente del Sistema para determinar su conformidad y eficacia, tanto del conjunto como de los controles individualmente vistos. La auditoría debe hacerse conforme a las técnicas vigentes, al plan de auditoría de la entidad y desde un enfoque basado en riesgos. En la Política para la Gestión Integral de Riesgos deben establecerse los criterios de auditoría que aplicaran al SIGRIP.
- d. Finalmente, la mejora del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP corresponde a la Alta Dirección o línea estratégica, quien lleva a cabo la revisión integral del Sistema. Este proceso de mejora debe ser continuo, y nutrirse de los reportes que se generan en el monitoreo, las evaluaciones y las auditorías. En todo caso se deben implementar los planes de mejoramiento que se requieran, para atender a los hallazgos y no conformidades identificadas por la auditoría. También, deben tenerse en cuenta, desde el enfoque preventivo, las evaluaciones y los resultados del monitoreo. En la Política para la Gestión Integral de Riesgos debe quedar definido el proceso de mejora continua del SIGRIP.

4.11. Articulación de la Gestión del Riesgo para Entidades Públicas vigiladas por la Superintendencia Nacional de Salud

Con el propósito de orientar el ejercicio de gestión integral de riesgos en entidades vigiladas del Sector Salud, cuyas entidades deben implementar el Sistema General de Seguridad

Social en Salud (SGSSS) que lidera el Ministerio de Salud y Protección Social, en la articulación con la supervisión basada en riesgos definida por la Superintendencia Nacional de Salud, mediante el anexo técnico denominado Lineamientos para la Articulación en la Gestión Integral del Riesgo para Entidades Públicas pertenecientes al Sistema de Seguridad Social en Salud, se establecen aquellos lineamientos comunes a las metodologías específicas que dichas entidades establecen, con el fin de incorporar elementos de análisis que, en todo caso serán complementarios a aquellos exigibles por dichos entes de control y vigilancia.

En este sentido, el documento que se encuentra en proceso de elaboración busca integrar los requerimientos de la Superintendencia Nacional de Salud, regulados mediante la Circular Externa 2022151000000053-5 de 2025 que define el Sistema Integral de Administración de Riesgos de Cumplimiento (SIARC), la Circular Externa 20211700000005-5 de 2021 sobre el Subsistema de Administración del Riesgo de Corrupción, Opacidad y Fraude (SICOF) y la Circular Externa 2022151000000053-5 de 2022 relacionada con el Programa de Transparencia y Ética Empresarial (PTEE), con el enfoque transversal de Gestión Integral del Riesgo promovido por el Departamento Administrativo de la Función Pública, en su Guía para la gestión integral del riesgo y el diseño de controles en entidades públicas – Versión 7.

Esta articulación resulta esencial para fortalecer el sistema de control interno, asegurar la eficiencia institucional y garantizar el cumplimiento normativo, a partir de la definición de un lenguaje común, criterios técnicos homogéneos y mecanismos efectivos de prevención y mitigación de riesgos, como eje fundamental para garantizar de forma razonable el buen uso de los recursos y el cumplimiento misional que eleve la capacidad de las entidades en la prestación de servicios a las ciudadanías.

Este anexo, por tanto, proporcionará lineamientos prácticos para identificar puntos de convergencia, evitar duplicidad de esfuerzos y avanzar hacia una gestión de riesgos sistemática, articulada y alineada con los objetivos estratégicos del sector salud y del Estado colombiano.

Nota: Este Anexo que desarrollará los Lineamientos para la Articulación en la Gestión Integral del Riesgo para Entidades Públicas pertenecientes al Sistema de Seguridad Social en Salud, se encuentra en proceso de elaboración en coordinación con el Ministerio de Salud y Protección Social, así como la Superintendencia Nacional de Salud, el cual será incluido en la caja de herramientas de forma posterior.

4.12. Seguimiento, Monitoreo y Revisión en el marco del Esquema de Líneas del Modelo Estándar de Control Interno MECI

Teniendo en cuenta el capítulo que desarrolla la alineación estratégica de la gestión del riesgo y el Modelo Integrado de Planeación y Gestión (MIPG), el cual a través de la Dimensión 6 despliega los componentes de evaluación del riesgo y actividades de control en articulación con el esquema de líneas, se precisa que dicho esquema atiende de manera íntegra la gestión del riesgo al interior de la entidad, comprometiendo todos los niveles de la organización, al definir los niveles de autoridad y responsabilidad en la aplicación de controles como eje para materializar el seguimiento y monitoreo a los riesgos que enfrenta la entidad, por lo que, se hace relevante definir adecuados mecanismos para la medición del riesgo como una herramienta estratégica que permite establecer la efectividad de los controles, validar el cumplimiento de metas, analizar comportamientos y tendencias, así como identificar posibles desviaciones que puedan afectar la gestión institucional.

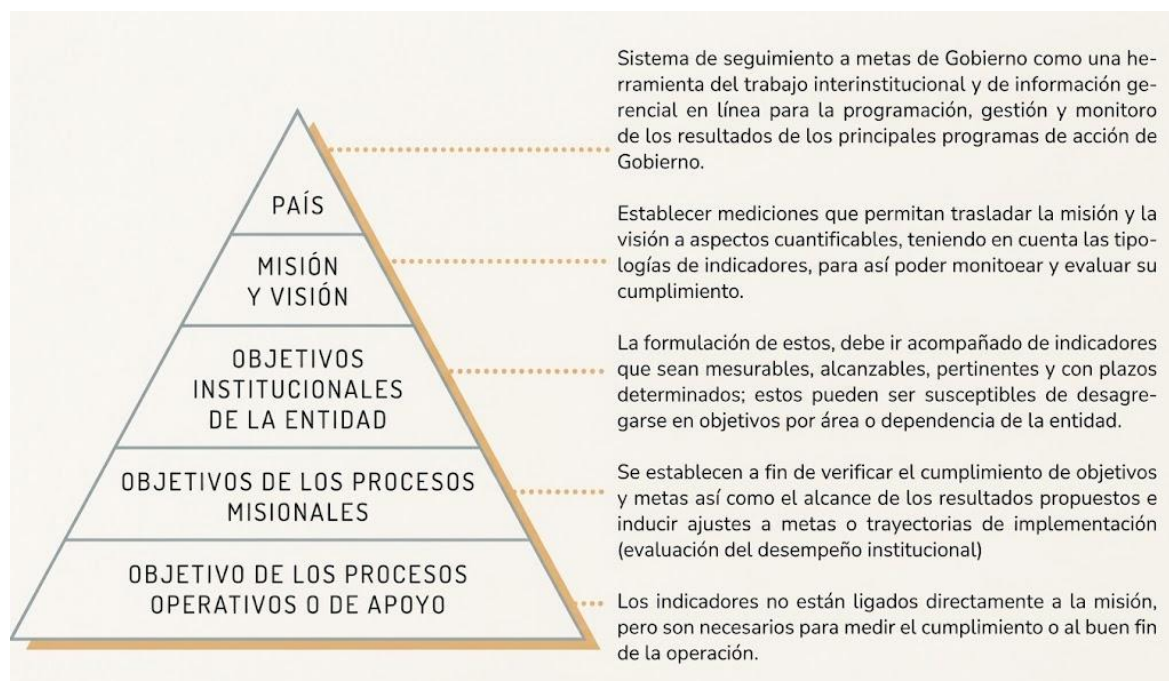
En este contexto, los Indicadores Clave de Riesgo (Key Risk Indicators – KRI por sus siglas en inglés), surgen como una herramienta fundamental para la toma de decisiones informadas de cara a la mitigación de riesgos, por lo que a continuación se precisan sus bases conceptuales y orientaciones técnicas para su diseño que dependerá de las características y complejidad de cada entidad.

4.12.1. Tipologías de Indicadores para el seguimiento

Con el propósito de definir de forma adecuada los Indicadores Clave de Riesgo, es necesario enmarcarlos desde el despliegue de la plataforma estratégica de la entidad, la cual parte de la misión, visión y valores fundamentales, base para la formulación de los objetivos estratégicos, los cuales a su vez, no solamente orientan la planeación institucional, sino que también, permiten tener un despliegue hacia los objetivos de los procesos y se constituyen en la base para la identificación y formulación de Indicadores Clave de Desempeño (Key Performance Indicators – KPI), que hacen posible medir su cumplimiento. Estos indicadores estarán referidos a aquellos que se diseñan para medir el cumplimiento misional, desde lo más estratégico hasta lo más operativo. Al respecto la Guía para la construcción y análisis de indicadores de gestión v4, señala lo siguiente:

Los indicadores se diseñan desde el proceso de planeación y permiten que durante las demás etapas de la gestión se verifique el cumplimiento de objetivos y metas, así como el alcance de los resultados propuestos e introducir ajustes a los planes de acción, metas o actividades. (Función Pública, 2018, p.12).

La misma guía, define los tipos de evaluación y los indicadores asociados, con una visión estratégica y el correspondiente despliegue hacia los procesos, programas y proyectos que desarrolla la entidad para su cumplimiento misional, tal como se observa en la siguiente figura.



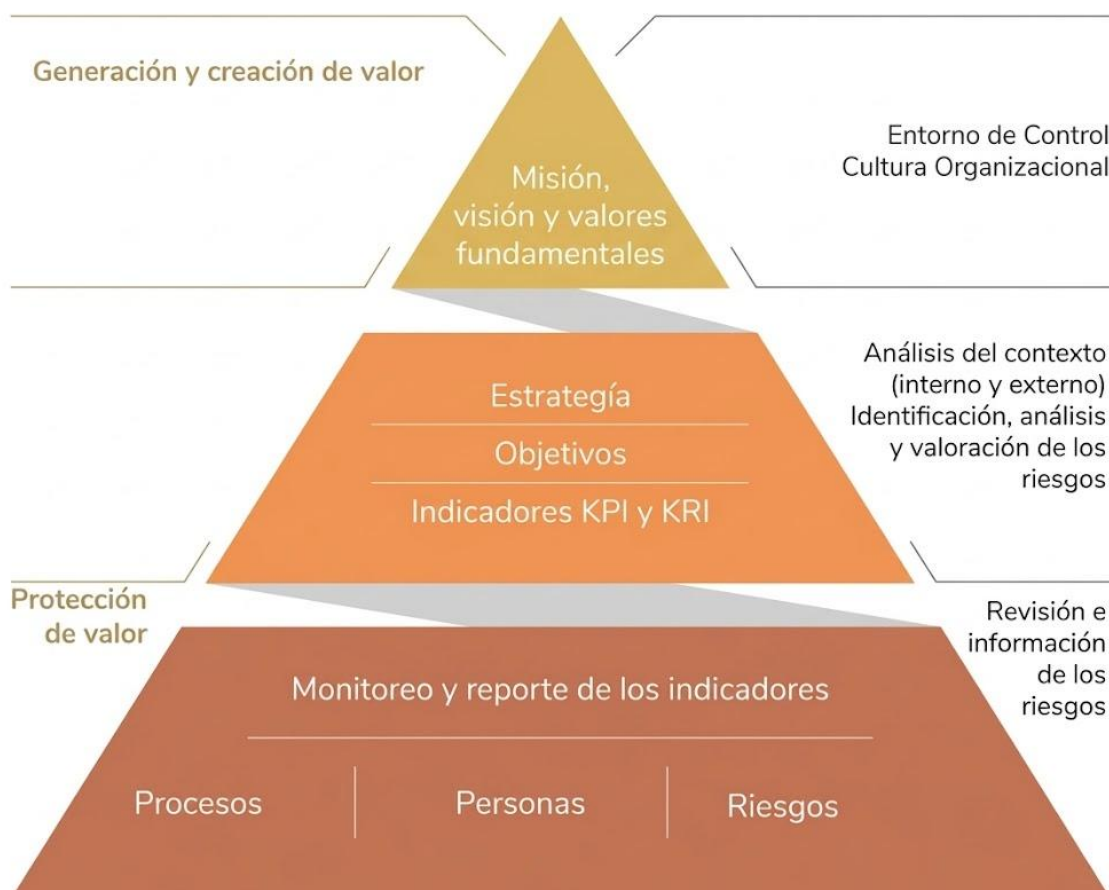
Fuente: Departamento Administrativo de la Función Pública, 2018

Se precisa entonces que, los Indicadores Clave de Riesgo (Key Risk Indicators- KRI), de acuerdo con el documento Desarrollo de Indicadores Clave de Riesgo para Fortalecer la Gestión de Riesgos Organizacional, emitido por el Committee of Sponsoring Organizations of the Treadway Commission (COSO), corresponden a:

“(…) métricas utilizadas por las organizaciones para proporcionar una señal temprana de exposiciones al riesgo, cada vez mayores en diversas áreas de la organización. (...) estos indicadores proporcionan información oportuna sobre riesgos emergentes y potenciales que pueden tener impacto sobre el logro de los objetivos de la organización, así como las medidas en las cuales diferentes eventos o puntos desencadenantes, pueden indicar problemas que se desarrollan internamente dentro de las operaciones de la organización o los riesgos potenciales relacionados con eventos externos, esto quiere decir que pueden ofrecer información valiosa para la administración y la junta directiva de cada organización para tomar las medidas correctivas y preventivas para mitigar los riesgos y velar por

el cumplimiento de los objetivos establecidos. (Citado por PricewaterhouseCoopers International, 2020, p.3).

En este sentido, de acuerdo con la estructura propuesta en la figura siguiente, se observa la forma como se vinculan los Indicadores Clave de Riesgo articulados con los Indicadores Clave de Proceso.



Fuente: Adaptado documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

Por lo tanto, estos indicadores tienen una función principal que es monitorear los riesgos clave que podrían afectar el cumplimiento de los objetivos y metas establecidos durante las diversas etapas de la gestión institucional. Así mismo, son fundamentales para realizar ajustes en la operación cuando sea necesario, lo que permite asegurar que los riesgos sean gestionados de forma adecuada y las decisiones se tomen a tiempo para mitigar cualquier desviación o amenaza.

4.12.2. Alcance de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI)

De acuerdo con la articulación explicada en el punto anterior, a continuación, se precisan los alcances en la aplicación de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI), ya que, si bien tienen diferencias, resultan complementarios en su análisis.

Indicadores Clave de Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
Permiten medir periódicamente el desempeño general de la entidad y sus principales unidades operativas.	Complementan el seguimiento a los resultados de la entidad.
Se definen tomando como referencia las metas establecidas, por procesos, unidades u operaciones clave.	Proporcionan una señal temprana y oportuna de una exposición al riesgo en diversas áreas de la entidad.
Mide el rendimiento pasado, proporcionando información sobre qué tan bien se están logrando los objetivos estratégicos y operativos.	Proporcionan información útil sobre los riesgos emergentes y potenciales que pueden impactar en los objetivos estratégicos de la organización.
Ofrecen información sobre aquellos aspectos críticos de la operación que requieren mayores recursos y atención.	Ayudan a identificar y anticipar problemas que se pueden presentar interna o externamente, así como oportunidades futuras.
Permiten medir los resultados que se obtienen de la ejecución de los programas, planes y proyectos, en los diferentes momentos o etapas de su desarrollo.	Permiten realizar un monitoreo constante y mitigar los posibles eventos de riesgo que se presenten al aplicar medidas oportunas para disminuir su impacto.
Permiten mejorar la planificación, entender con mayor precisión las oportunidades de mejora de determinados procesos y analizar el desempeño de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad.	Facilitan el proceso de generación de informes y el escalamiento de los riesgos.

Fuente: Adaptado documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

4.12.3. Lineamientos generales para el establecimiento de Indicadores clave de riesgo (KRI)

Para lograr una adecuada comprensión de esta tipología de indicadores, es importante retomar la definición general ya citada en el punto anterior, donde el COSO precisa que se trata de “métricas utilizadas por las organizaciones para proporcionar una señal temprana de exposiciones al riesgo”. Este mismo comité a través de la estructura para el modelo COSO-ERM señala sobre estos indicadores:

“(…) se utilizan para predecir la ocurrencia de un riesgo, generalmente son de carácter cuantitativo, pero también pueden ser cualitativos. Los indicadores clave se comunican a los niveles de la entidad que están en mejor posición para gestionar el riesgo emergente cuando sea necesario. Deberían comunicarse junto con los indicadores clave de desempeño (KPI’s) para demostrar la interrelación entre el riesgo y el desempeño. Los indicadores clave facilitan un enfoque proactivo de la gestión del desempeño. (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.107).

Por su parte, la Universidad Internacional de La Rioja (2024) explica que:

“(…) los indicadores claves de riesgo (KRI), son métricas diseñadas con el propósito de identificar y monitorear posibles amenazas que puedan afectar el cumplimiento de los objetivos de una organización. Implementarlos facilita una gestión proactiva de los riesgos, ya que proporciona información valiosa sobre tendencias o patrones que podrían indicar la aparición de problemas. Al monitorear estos indicadores, las empresas pueden ajustar su estrategia de mitigación de riesgos o de procesos, a fin de minimizar posibles impactos adversos. Para ello, es vital que las métricas estén alineadas con los objetivos y contextos de cada organización”.

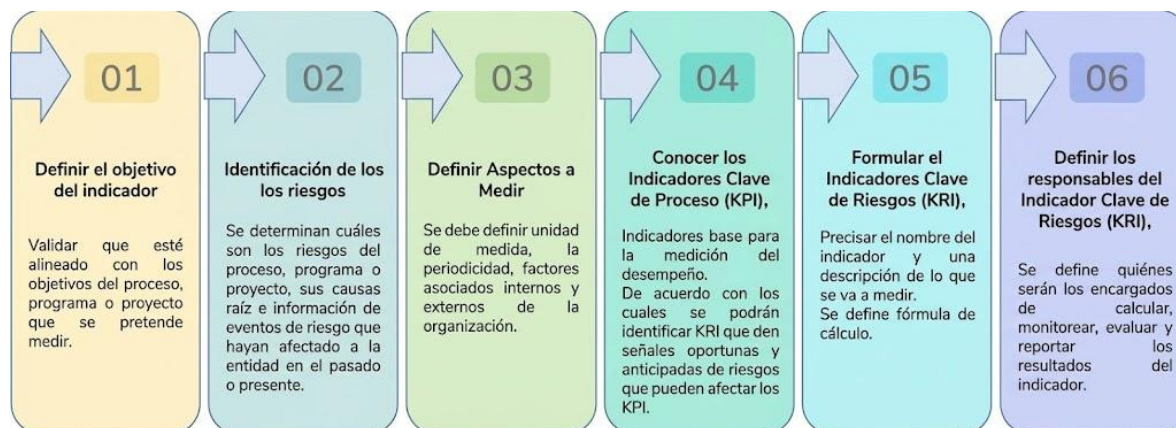
Así mismo, Delfiner y Pailhé (2008) indican que los KRI son herramientas para estimar la probabilidad y severidad de eventos, pudiendo ser de carácter cualitativo o cuantitativo y expresarse en porcentajes, cantidades o montos. Además, señalan ciertos atributos deseables en los KRI, como es que permitan medir y controlar un riesgo, y que, permitan generar actividades preventivas para minimizar pérdidas, y detectar tendencias o cambios en los niveles de riesgo.

Atendiendo estas conceptualizaciones, se puede establecer que los Indicadores Clave de Riesgos (KRI), son métricas diseñadas con el fin de identificar, estimar y monitorear la ocurrencia y severidad de eventos y posibles amenazas que puedan llegar a afectar el cumplimiento de los objetivos institucionales en los diferentes niveles, por lo que se constituyen en la herramienta para el seguimiento y monitoreo de los riesgos, ya que pueden entregar señales de alerta temprana, así como detectar tendencias o cambios en los niveles de riesgo, lo que facilita que se incorporen acciones correctivas y preventivas para minimizar sus impactos frente a posibles materializaciones.

Los Indicadores Clave de Riesgos (KRI), hacen referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No necesariamente

indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe analizar.

Estos indicadores permiten registrar la ocurrencia de un evento que se asocia a un riesgo identificado previamente, lo cual permite llevar un registro de eventos y evaluar a través de su tendencia la efectividad de los controles que se disponen para mitigarlos. Para la definición y construcción de los Indicadores Clave de Riesgos (KRI), se proponen los siguientes pasos que se despliegan a continuación.



Fuente: Adaptado de Documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo y Pirani Risk, Guía Práctica Indicadores Clave de Riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

Para el desarrollo de los anteriores pasos se debe tener en cuenta:

1. Definir el objetivo del indicador, el cual debe estar alineado con los objetivos del proceso, plan, programa o proyecto que se pretende medir.
2. Identificar los riesgos, en este paso se determinan cuáles son los riesgos del proceso, plan, programa o proyecto, sus causas raíz e información de eventos de riesgo que hayan afectado a la entidad en el pasado o presente.

Sobre la gestión de eventos, se trata de un riesgo materializado, donde se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente. Algunas fuentes para establecer una base histórica de eventos pueden ser: i) mesas de ayuda; ii) PQRD (peticiones, quejas, reclamos, denuncias); iii) Oficina jurídica; iv) Líneas internas y externas de denuncia.

3. Definir los aspectos a medir, para lo cual se deben establecer la unidad de medida, la periodicidad, los factores internos o externos de la entidad y especialmente, que se pretende medir.
4. Conocer los Indicadores Clave de Proceso (KPI), teniendo en cuenta que estos son la base de medición del desempeño del proceso, programa o proyecto.
5. Formular el Indicador Clave de Riesgo (KRI), se debe precisar como mínimo lo siguiente:
 - i. El nombre del indicador,
 - ii. una descripción de lo que se va a medir,
 - iii. la fórmula de cálculo,
 - iv. La fuente de información para el cálculo del indicador, por ejemplo: sistemas internos, reportes de auditoría, bases de datos internas y/o externas u otras fuentes,
 - v. frecuencia de medición y seguimiento y;
 - vi. umbrales de alerta.

Algunos ejemplos de indicadores se presentan a continuación:

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos
		% solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

En este punto se deben establecer los umbrales de alerta, ya que no todos los cambios en los KRI requieren acción inmediata, por lo que, es fundamental que el líder del proceso, plan, programa o proyecto defina los umbrales de alerta que señalen cuándo un KRI alcanza un nivel que requiere atención, lo que permite a la entidad priorizar las áreas que necesitan intervención inmediata y distinguirlas de aquellas situaciones donde los riesgos están bajo control.

Para este efecto, para cada KRI se debe definir una semaforización que permita distinguir entre valores aceptables, riesgosos o críticos, así:

- Valor Bajo (Verde): Valor mínimo deseado
- Valor Moderado (Amarillo): Valor que indica riesgo potencial
- Valor Alto (Rojo): Valor crítico o inaceptable

Estos valores dependerán del proceso, plan, programa o proyecto que se esté analizando y de sus indicadores clave de desempeño.

Ahora bien, es fundamental comprender que el resultado del cálculo del KRI se relaciona directamente con el apetito al riesgo, y debe ser analizado de cara a la declaración de apetito de la entidad bajo las siguientes consideraciones.

- i. Valor del KRI dentro del apetito al riesgo: Significa que la operación de la entidad, y por ende el riesgo se sigue moviendo dentro de lo que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.
 - ii. Valor del KRI que excede el apetito al riesgo: Significa que el riesgo ha superado el umbral que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. En este caso se deben tomar acciones correctivas o de mitigación para llevar el riesgo de nuevo hacia un rango tolerable.
 - iii. Valor del KRI se acerca al umbral de alerta definido: Revela que el riesgo se ha ido aumentando y que podría salir del umbral de alerta si continua así.
6. Definir los responsables del Indicador Clave de Riesgos (KRI), será necesario definir quiénes serán los encargados de calcular, monitorear, evaluar y reportar los resultados del indicador.

Algunas recomendaciones a tener en cuenta para identificar y formular los Indicadores Clave de Riesgo (KRI) para una mayor efectividad se señalan a continuación:

- Relevancia: Deben estar alineados con los riesgos críticos para la entidad.
- Cuantificables: Es fundamental que los Indicadores Clave de Riesgo (KRI) puedan ser medidos de manera objetiva.
- Predictivos: Un buen Indicador Clave de Riesgo (KRI) debería ser capaz de predecir o bien detectar posibles problemas antes de que ocurran.
- Comparables: Los Indicadores Clave de Riesgo (KRI) deben permitir la comparación a lo largo del tiempo para identificar tendencias.

- En cuanto a las limitaciones que pueden presentarse en el diseño de estos indicadores se tienen las siguientes:
- Un Indicador Clave de Riesgo (KRI) no sustituye la comprensión integral del contexto de la entidad, es decir, se requiere un conocimiento del entorno y las características de la entidad para diseñar y medir estos indicadores.
- Si la fuente de información (interna o externa) no es confiable porque esta desactualizada, es errada y/o no posee un histórico de datos podría ocasionar Indicadores Clave de Riesgo (KRI) ineficientes.
- Si presentan fallas en el establecimiento de los umbrales de los Indicadores Clave de Riesgo (KRI) puede generar que no se ajusten las estrategias de la entidad de manera proactiva y puede disminuir la probabilidad del cumplimiento de las metas y objetivos institucionales.

4.12.4. Comunicación y reporte KRI en el marco del esquema de líneas de aseguramiento

En concordancia con lo dispuesto en el Esquema de Líneas de Aseguramiento, eje articulador para la política de control interno, Dimensión 7 de MIPG, para los Indicadores Clave de Riesgo (KRI) por su enfoque preventivo, y que se articulan a los Indicadores Clave de Proceso (KPI), se requiere para cada uno de los roles identificados un trabajo conjunto para contribuir colectivamente a la generación de alertas tempranas, con el fin de fortalecer la gestión del riesgo y evitar su materialización.

Por lo expuesto, se propone el siguiente esquema de asignación de roles y responsabilidades que se distribuyen en diversos servidores de la entidad y mantiene la dinámica que ha propuesto para el esquema de líneas de aseguramiento. Este despliegue es un referente y podrá adaptarse a las necesidades y complejidad de cada entidad

Líneas de aseguramiento	Responsable	Responsabilidad frente a los Indicadores Clave de Riesgo (KRI)
Línea Estratégica	Alta Dirección Comité institucional de coordinación de control interno / instancia similar del mismo nivel	• Incorporar en la política para la gestión integral de riesgos lineamientos sobre los Indicadores Clave de Riesgo (KRI)
		• Realizar seguimiento y análisis periódico a los indicadores claves de riesgos institucionales y proponer mejoras a su estructura.
		• Analizar los umbrales definidos para los Indicadores Clave de Riesgo (KRI) y sugerir ajustes de ser necesario, de tal forma que estos se alineen con los niveles aceptables para la entidad.
		• Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a

Líneas de aseguramiento	Responsable	Responsabilidad frente a los Indicadores Clave de Riesgo (KRI)
		los indicadores claves de riesgo, así como a los indicadores clave de proceso asociados.
	Comité de Gestión y Desempeño Institucional	• Realizar seguimiento y análisis periódico a los indicadores claves de desempeño de manera articulada con los indicadores clave de riesgo. • Generar las alertas que correspondan, de acuerdo con los umbrales definidos para los Indicadores Clave de Riesgo (KRI)
1ª Línea de Aseguramiento	Líderes de Procesos Responsable del proyecto Servidores en general	• Identificar y formular los indicadores clave de riesgos que pueden alertar sobre la exposición al riesgo para los procesos, programas o proyectos bajo su responsabilidad.
		• Aplicar, medir y hacer seguimiento a los indicadores clave de riesgos, alineados con los indicadores clave de proceso.
		• Reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos de acuerdo con los indicadores claves de riesgo dentro de los plazos establecidos.
		• Informar a la Oficina Asesora de Planeación o quien haga sus veces (como 2ª línea de defensa) sobre las alertas críticas resultado de la medición de los indicadores claves de riesgo bajo su responsabilidad.
		• Si se identifica que un indicador claves de riesgo está fuera del umbral esperado, la primera línea de defensa debe actuar para corregir las desviaciones identificadas.
		• Establecer y aplicar las acciones de mejora requeridas para optimizar la operación de los procesos, planes, programas o proyectos de acuerdo con los resultados de las métricas aplicadas.
2ª Línea de Aseguramiento	Oficina Asesora de Planeación, Gerencias de Riesgos o quien haga sus veces	• Asegurar que los indicadores claves de riesgo estén alineados con los objetivos estratégicos y operativos de la entidad.
		• Proponer la inclusión de los lineamientos en materia de indicadores claves de riesgo en la estructura de la política para la gestión integral de riesgos, para aprobación por parte de la Alta Dirección.
		• Establecer las metodologías que guíen la medición, seguimiento y monitoreo de los indicadores claves de riesgo, asegurando que se utilicen las mejores prácticas y se implementen de manera efectiva.
		• Consolidar los indicadores claves de riesgo con mayor criticidad frente al logro de los objetivos y presentarlos periódicamente (establecer una periodicidad concreta) ante la Línea Estratégica para su análisis y toma de decisiones.

Líneas de aseguramiento	Responsable	Responsabilidad frente a los Indicadores Clave de Riesgo (KRI)
		• Asesorar y supervisar a la 1ª línea para la correcta identificación, formulación e implementación de los indicadores claves de riesgo.
3ª Línea de Aseguramiento	Jefe Oficina Asesora de Control Interno o quien haga sus veces	• Verificar si los indicadores claves de riesgo están definidos y se aplican por parte de los responsables.
		• Evaluar si los indicadores claves de riesgo son pertinentes y eficaces para la oportuna generación de alertas y/o implementación de correctivos.
		• Informar a la Alta Dirección en coordinación con la 2ª línea, cuando se detecten deficiencias o brechas en los indicadores claves de riesgo para que tomen decisiones sobre las medidas preventivas y correctivas que deben implementarse.
		• Asesorar y acompañar a la Alta Dirección en el análisis de los resultados de los indicadores claves de riesgo, así como en la incorporación de estrategias para la identificación y monitoreo estratégico de los indicadores claves de riesgo.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

REFERENCIAS

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 7. Dirección de Gestión y Desempeño Institucional. 2025.

Instituto de Auditores Internos/ PricewaterhouseCoopers. PwC. COSO Committee of Sponsoring Organizations of the Treadway Commission. (2017). Gestión del riesgo empresarial, integrando estrategia y desempeño.

Fundación Latinoamericana de Auditores Internos FLAI. The Institute of Internal Auditors, Inc. Perspectivas y percepciones globales, Gobernanza, riesgo y control. (2023). Universidad del Rosario. (2020). Curso Riesgo Operativo.

Organización Internacional de Normalización (ISO). (2018). ISO 31000. Gestión del riesgo. Directrices.

Instituto de Auditores Internos de España. (2013). Fábrica de Pensamiento. Definición e implantación de apetito del riesgo. <https://auditoresinternos.es/centro-de-conocimiento/fabrica-de-pensamiento/>

Instituto de Auditores Internos de España. (2021). Fábrica de Pensamiento. Auditoría Interna y gestión de riesgos. <https://auditoresinternos.es/centro-de-conocimiento/fabrica-de-pensamiento/>

Superintendencia Financiera de Colombia. Apetito del riesgo, guía externa. <https://www.superfinanciera.gov.co/loader.php?IServicio=Tools2&ITipo=descargas&IFuncion=descargar&idFile=1072547>

Departamento Administrativo de la Función Pública. (2020). Guía para la gestión por procesos en el marco de MIPG.

PwC. (2020). Indicadores claves de riesgo. <https://www.pwc.com/ve/es/publicaciones/assets/PublicacionesNew/Boletines/Indicadores%20claves%20de%20riesgo-oct2020.pdf>

Control de Cambios

VERSIÓN	FECHA	ELABORADO POR	REVISADO POR	APROBADO POR	OBSERVACIONES
1	23/06/2021	Alvaro Gamboa Rojas Encargado de Calidad	Comité Coordinador de Control Interno	Acta No. 003- 2021 Comité Institucional de Gestión y Desempeño	Creación del documento.
2	30/08/2023	Alvaro Gamboa Rojas Encargado de Calidad	Comité Coordinador de Control Interno	Acta No. 003- 2023 Comité Institucional de Gestión y Desempeño	Creación del documento.
3	28/09/2026	Oscar Dario Gomez Chacon Gestión de Planeación Institucional	Comité Institucional de Gestión y Desempeño	Acta No. 010- 2026 Comité Institucional de Gestión y Desempeño	Actualización del documento.

RESOLUCIÓN N° 00940

Veintiocho (28) de Septiembre Dos Mil Veintiséis (2026)

"POR LA CUAL SE ADOPTA E IMPLEMENTA LA POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO EN EL SANATORIO DE CONTRATACIÓN ESE"

LA GERENTE DEL SANATORIO DE CONTRATACIÓN E.S.E.

En uso de sus facultades Constitucionales, legales y en especial por las conferidas por los Decretos N° 1289 de 1994, modificado parcialmente por el Decreto 1502 de 2023 y las demás normas concordantes y concomitantes y;

CONSIDERANDO:

Que la Constitución Política de Colombia, en su artículo 209, establece que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad.

Que el artículo 269 de la Carta Política señala que en las entidades públicas las autoridades correspondientes están obligadas a diseñar e aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley.

Que la Ley 87 de 1993, por la cual se establece el Sistema de Control Interno en las Entidades y Organismos del Estado, determina como uno de sus objetivos específicos el establecimiento de mecanismos institucionales para la identificación y prevención de riesgos.

Que el artículo 4 del Decreto 1537 de 2001 define la Administración Riesgos como parte integral del fortalecimiento de los Sistemas de Control Interno en las entidades públicas, para lo cual se establecerán y aplicarán políticas de administración del riesgo.

Que el Decreto 1599 de 2005 estableció el Modelo Estándar de Control Interno MECI 1000:2005 para las Entidades Públicas, y en él se establece como componente prioritario el sistema de administración de riesgos.

Que el Decreto 1011 de 2006 en su artículo 6° establece como uno de los objetivos principales del Sistema Único de Habilitación, del Sistema Obligatorio de la Calidad para la Atención en Salud del Sistema General de Seguridad Social en Salud, la protección a los usuarios frente a los potenciales riesgos asociados a la prestación de los servicios de salud.

Que el Decreto 1499 de 2017 actualizó el Modelo Integrado de Planeación y Gestión (MIPG), el cual integra el Sistema de Gestión y el Sistema de Control Interno, articulando la dimensión de "Direccionamiento Estratégico y Planeación" y la dimensión de "Control Interno" (a través del Modelo Estándar de Control

CONTINUA RESOLUCIÓN N° 00940 DE VEINTIOCHO (28) DE SEPTIEMBRE DE DOS MIL VEINTISÉIS (2026) "POR LA CUAL SE ADOPTA E IMPLEMENTA LA POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO EN EL SANATORIO DE CONTRATACIÓN ESE".

Interno - MECI), las cuales **exigen** una administración activa y transversal del riesgo.

Que el artículo 1 del Decreto 1122 de 2024 modificó el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 (Decreto Reglamentario Único del Sector Presidencia de la República) y dispuso que las entidades públicas del orden nacional deben implementar Programas de Transparencia y Ética Pública bajo los estándares, requisitos y controles establecidos por la Secretaría de Transparencia de la Presidencia de la República.

Que el Departamento Administrativo de la Función Pública (DAFP) expidió la "Guía para la Gestión Integral del Riesgo en Entidades Públicas" (Versión 7), alineada con el estándar internacional COSO-ERM (2017), la cual redefine las directrices para la identificación, evaluación, tratamiento y monitoreo de los riesgos en el sector público, exigiendo la formalización del apetito de riesgo y la clasificación obligatoria de tipologías como riesgos estratégicos, operativos, de integridad (corrupción), seguridad digital, fiscales y emergentes.

Que el Sanatorio de Contratación ESE, como Entidad Social del Estado del orden nacional, requiere actualizar y formalizar su Política de Gestión Integral del Riesgo para garantizar la continuidad en la prestación de los servicios de salud, salvaguardar sus recursos, asegurar el cumplimiento de sus fines misionales y fortalecer una cultura institucional de prevención y autocontrol.

Que el Comité Institucional de Gestión y Desempeño del Sanatorio de Contratación ESE, en sesión del 28 de septiembre de 2026, aprobó el documento denominado Política de Gestión Integral del Riesgo del Sanatorio de Contratación ESE.

Que, por lo antes expuesto, la Gerente del SANATORIO DE CONTRATACIÓN E.S.E,

R E S U E L V E:

ARTÍCULO 1º.- ADOPCIÓN. Adoptase la Política Institucional de Gestión Integral del Riesgo del Sanatorio de Contratación E.S.E., contenida en el documento anexo que hace parte integral del presente acto administrativo.

El Sanatorio de Contratación ESE, se compromete a mantener bajo control los riesgos generales de gestión, fiscales, de seguridad de la información, para la integridad pública y los establecidos para las entidades vigiladas por la Superintendencia Nacional de Salud, mediante la aplicación del manual y metodología institucional. A través de controles preventivos y detectivos oportunos, la entidad busca evitar que las amenazas se concreten, corregir desviaciones y minimizar cualquier impacto negativo en sus diferentes procesos, para salvaguardar la integridad institucional.

CONTINUA RESOLUCIÓN N° 00940 DE VEINTIOCHO (28) DE SEPTIEMBRE DE DOS MIL VEINTISÉIS (2026) "POR LA CUAL SE ADOPTA E IMPLEMENTA LA POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO EN EL SANATORIO DE CONTRATACIÓN ESE".

ARTÍCULO 2°.- ALCANCE. Esta política es vinculante y de aplicación obligatoria para todos los procesos institucionales (estratégicos, misionales, de apoyo y de evaluación y control), planes, programas, proyectos, y para las acciones ejecutadas por los servidores públicos y contratistas del Sanatorio de Contratación ESE en el desarrollo de sus funciones.

ARTÍCULO 3°.- TIPOLOGÍAS DE RIESGO. En consonancia con la Versión 7 de la Guía del DAFP, el Sanatorio administrará el riesgo bajo un enfoque integral que unifica criterios para las siguientes tipologías específicas:

- a. Riesgos Estratégicos: Eventos que impactan directamente el direccionamiento y las metas de largo plazo de la ESE.
- b. Riesgos Operativos: Fallas o deficiencias asociadas al talento humano, deficiencias en los procesos de salud o administrativos, tecnología e infraestructura.
- c. Riesgos de Integridad Pública (Corrupción): Conductas que desvíen la finalidad de la función pública para obtener beneficios particulares, articulados con el Plan de Transparencia y Ética Pública.
- d. Riesgos de Seguridad Digital (Seguridad de la Información): Amenazas y vulnerabilidades tecnológicas que pongán en peligro los activos de información, historias clínicas y datos sensibles de los usuarios (en articulación con MinTIC).
- e. Riesgos Fiscales: Situaciones que puedan generar impactos negativos y detrimento de los recursos financieros y patrimoniales de naturaleza pública asignados a la institución.
- f. Riesgos Emergentes: Identificación de nuevas amenazas relacionadas con la transformación digital, ciberseguridad, sostenibilidad ambiental y cambios en el entorno de la salud pública.
- g. Riesgo en salud: Concebido como el impacto negativo, de un suceso adverso en los determinantes sociales, ambientales y económicos, que actúan sobre el bienestar individual o colectivo, alterando la expectativa de vida saludable en las poblaciones afectadas y de influencia de la Entidad.

ARTÍCULO 4°.- ROLES Y RESPONSABILIDADES. La gestión integral del riesgo en la entidad se estructurará bajo el modelo de Líneas de Defensa.

Línea estratégica

La Alta Dirección de la ESE (El Gerente y su equipo directivo)
El Comité Institucional de Coordinación de Control Interno

Funciones: Definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual

CONTINUA RESOLUCIÓN N° 00940 DE VEINTIOCHO (28) DE SEPTIEMBRE DE DOS MIL VEINTISÉIS (2026) "POR LA CUAL SE ADOPTA E IMPLEMENTA LA POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO EN EL SANATORIO DE CONTRATACIÓN ESE".

toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.

Primera línea de defensa

Líderes de procesos, programas y proyectos y sus equipos
Los servidores públicos de todos los niveles de la ESE

Funciones: Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo).

Segunda línea de defensa

Jefe de la Oficina de Planeación
Comité de compras
Encargado TIC
Responsables de temas transversales para toda la entidad y que reporta ante el Representante Legal

Funciones: Hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora de este tema.

Tercera línea de defensa

Oficina de Control Interno

Funciones: A través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación.

ARTÍCULO 6°.- ADOPCIÓN MANUAL DE GESTIÓN INTEGRAL DEL RIESGO. Adoptase el Manual de Gestión Integral del Riesgo del Sanatorio de Contratación E.S.E., contenido en el documento anexo que hace parte integral del presente acto administrativo.

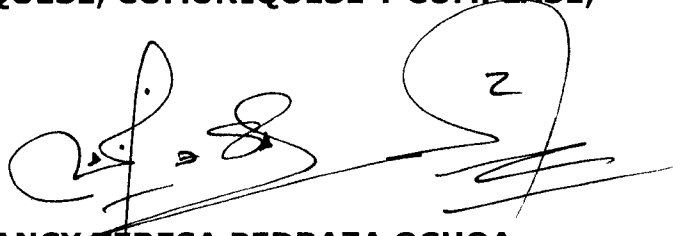
ARTÍCULO 7°.- MONITOREO Y SEGUIMIENTO. Los líderes de cada proceso deberán revisar y actualizar sus mapas de riesgo de manera periódica. La Segunda Línea de Defensa consolidará los informes de seguimiento de forma cuatrimestral para la toma de decisiones de la Alta Dirección, sin perjuicio de las evaluaciones independientes que realice la Oficina de Control Interno.

CONTINUA RESOLUCIÓN N° 00940 DE VEINTIOCHO (28) DE SEPTIEMBRE DE DOS MIL VEINTISÉIS (2026)
"POR LA CUAL SE ADOPTA E IMPLEMENTA LA POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO EN EL SANATORIO
DE CONTRATACIÓN ESE".

ARTÍCULO 8°.- VIGENCIA. La presente resolución rige a partir de la fecha de publicación y deroga todas las disposiciones que le sean contrarias, especial la Resolución N° 0508 de 2021.

Dada en Contratación Santander, a los veintiocho (28) días del mes de septiembre de dos mil veintiséis (2026).

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE;



NANCY TERESA PEDRAZA OCHOA
Gerente Sanatorio de Contratación ESE

Proyectó: Óscar Darío Gómez Chacón. Oficina de Planeación SCESE
Aprobó: Nancy Teresa Pedraza Ochoa. Gerente SCESE



