Función Pública

Guía para la Gestión Integral del Riesgo en Entidades Públicas

Versión 7

Departamento Administrativo de la Función Pública
Mariella Barragán Beltrán
Directora
Equipo Trabajo:
Luz Daifenis Arango Rivera
Directora de Gestión y Desempeño Institucional
Iván Arturo Márquez
Myrian Cubillos
Carmen Julia Páez Villamil
Ana Yolanda Garzón
Elisa Fernanda Morales
Carlos Andres Rodriguez

Secretaria de Transparenciade la Presidencia de la República
Andrés Idárraga Franco
Secretario de Transparencia
Equipo Trabajo
Hernán Ramiro Amaya Guevara
Hernando Omar Toledo Valencia

Ministerio Tecnologias de la Información y Comunicaciones
Julián Molina Gómez
Ministro
Equipo Trabajo
Luis Clímaco Córdoba Gómez
Danny Alejandro Garzón Aristizábal
Johanna Marcela Forero Varela

Ministerio de Salud y Protección Social
Guillermo Alfonso Jaramillo
Ministro
Equipo Trabajo
Iván Javier Angarita Gálvez
Luz Adriana Zuluaga Salazar

Superintendencia Nacional de Salud
Helver Giovanni Rubiano García
Superintendente Nacional de Salud
Equipo Trabajo
Kevin Alberto Chaverra

Carrera 6 no. 12_62
Bogotá D.C., Colombia
www.funcionpublica.gov.co
eva@funciopublica.gov.co
Teléfono: (601) 7395656

Control de cambios al documento

Versión	Observación
Versión 1 **Mayo de 2009**	Creación Documento, basados en la Norma Técnica NTC5254
Versión 2 **Septiembre de 2011**	Se mantiene estructura conceptual, se actualizan lineamientos, acorde con la Norma ISO31000.
Versión 3 **Octubre de 2014**	Se mantiene estructura conceptual, se mejora visualmente mediante la inclusión de esquemas explicativos de los contenidos. Alineación con políticas de lucha contra la corrupción.
Versión 4 **Octubre de 2018**	Se mantiene estructura conceptual, se articulan las políticas de lucha contra la corrupción y seguridad de la información. Se define metodología para el diseño de controles.
Versión 5 **Noviembre de 2020**	Se mantiene estructura conceptual, con precisiones en los siguientes aspectos: 1. Ajustes en definición riesgo y otros conceptos relacionados con la gestión del riesgo. Se articula la institucionalidad de MIPG con la gestión del riesgo. 2. En paso 1: identificación del riesgo, se estructura propuesta para la redacción del riesgo. 3. Se amplían las tipologías de riesgo. 4. En paso 2 valoración del riesgo: se precisa análisis de probabilidad e impacto y sus tablas de referencia, así como el mapa de calor resultante. 5. Para el diseño y evaluación de los controles se ajusta tabla de calificación. 6. Se reubica y precisan las opciones de tratamiento del riesgo. 7. Se incluyen indicadores clave de riesgo. 8. Se precisan términos y uso relacionados con los planes de tratamiento del riesgo. 9. Se incluye en la caja de herramientas una matriz para el mapa de riesgos. 10. Se amplía el alcance de la seguridad digital a la seguridad de la información.

Versión	Observación
Versión 6 **Noviembre de 2022**	Se mantiene estructura conceptual para la administración del riesgo. Se incluye capítulo específico sobre riesgo fiscal, que se complementa con el Anexo denominado catalogo indicativo de puntos de riesgo fiscal para facilitar el análisis en el marco del modelo de operación por procesos.
Versión 7 **Agosto de 2025**	1. Se mantiene estructura conceptual y metodológica general para la gestión del riesgo bajo un enfoque integral, atendiendo las políticas de gestión y desempeño que se vinculan y su relación con otras políticas públicas y los sectores que las lideran. Se define estructura general para la gestión integral del riesgo, con elementos comunes aplicables a todas las tipologías de riesgo. 2. Se amplían términos y definiciones en concordancia con las actualizaciones en los capítulos, los cuales se desarrollan como anexo de la presente guía. 3. Se incluyen contenidos del marco COSO-ERM (2017) que precisan y profundizan los conceptos de riesgo, gestión del riesgo y niveles de madurez del riesgo. En este marco general se profundiza el análisis sobre apetito del riesgo. 4. Se precisan contenidos conceptuales y ejemplos relacionados con la gestión preventiva de riesgos fiscales. Se actualizan ejemplos con el despliegue metodológico establecido. 5. Se modifica y actualiza el capítulo relacionado con riesgos asociados a posibles actos de corrupción, mediante la incorporación del Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP, de acuerdo con el componente programático denominado Estrategia Institucional para la Lucha Contra la Corrupción, temática 1 Administración del Riesgo desplegado en el Anexo Técnico de los Programas de Transparencia y Ética Pública. 6. Se actualizan contenidos relacionados con los riesgos de seguridad de la información, desplegando la totalidad de los pasos metodológicos y se incluye una matriz que desarrolla un ejemplo práctico como anexo. 7. Se actualiza la caja de herramientas, de acuerdo con los temas que se incorporan.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Introducción

El Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, en articulación con la Secretaría de Transparencia y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) pone a disposición de las entidades la metodología para la gestión integral del riesgo, la cual se actualiza con 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, temática 1 Administración del Riesgo desplegado en el Anexo Técnico de los Programas de Transparencia y Ética Pública, en cumplimiento de lo establecido en la Ley 2195 de 2022[1] y el Decreto 1122 de 2024[2], reglamentación que modifica el capítulo relacionado con riesgos asociados a posibles actos de corrupción descrito en la versión 6 de la guía. De igual forma, en materia de seguridad de la información se incluyen las actualizaciones pertinentes para la gestión de estos riesgos de forma articulada, de acuerdo con esquema metodológico general.

Complementariamente, en coordinación con el Ministerio de Salud y Protección Social y la Superintendencia Nacional de Salud se desarrolla un anexo técnico que busca orientar a las entidades públicas pertenecientes al Sistema General de Seguridad Social en Salud (SGSSS), frente a la articulación de los lineamientos emitidos por dichas entidades en materia de riesgos y lo establecido en la presente guía, lo que les permitirá establecer aquellos aspectos comunes para su implementación, atendiendo la complejidad del sector y la criticidad en aspectos clave de su operación.

Así mismo, esta actualización recoge algunos de los principios que componen el modelo COSO ERM – Gestión de riesgos empresariales, conocido como el principal referente mundial en materia de gestión de riesgos, emitido por el Comité de Organizaciones

[1] Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.
[2] Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública

Patrocinadoras de la Comisión *Treadway* (COSO) en su última versión de 2017. Esta incorporación busca fortalecer aspectos referentes a la buena Gobernanza de la gestión de riesgos en las entidades y promover la adopción paulatina de estándares internacionales de reconocido valor técnico y extendida aplicación en este ámbito.

La presente actualización incluye, igualmente, la mejora en las estructura de ejemplos planteados en el capítulo de riesgos fiscales, a partir de la implementación de este tema en las entidades; se precisan algunos aspectos metodológicos y de articulación en el marco del Modelo Integrado de Planeación y Gestión MIPG y de la Dimensión de Control Interno, con el fin de orientar a las entidades para que en su implementación se aplique una visión sistémica para la gestión del riesgo, así como para involucrar el monitoreo y evaluación desde una perspectiva preventiva.

Dada la diversidad de entidades que se desenvuelven en sectores regulados, se incorpora un anexo que articula los requerimientos y reglamentación emitida por parte de la Superintendencia Nacional de Salud como instancia de vigilancia y control en materia de salud, para que las entidades prestadoras de servicios de salud vinculen elementos clave para el seguimiento y monitoreos integrales. Así mismo, se tienen en cuenta los lineamientos establecidos por parte del Ministerio de Salud y Protección Social para las Secretarías de Salud en entidades del nivel territorial, con el fin de facilitar a este tipo de entidades la gestión integral de riesgos atendiendo sus particularidades y misionalidad.

En este marco general, en el capítulo I se establecen los elementos de articulación para una efectiva gestión del riesgo, en desarrollo del Modelo Integrado de Planeación y Gestión (MIPG), donde se analizan las políticas de gestión y desempeño institucional, necesarias para viabilizar la aplicación del marco para la gestión integral del riesgo que define la presente guía.

Enseguida en el Capítulo II se desarrollan aspectos clave necesarios que habilitan el esquema metodológico propuesto, desde el fortalecimiento de una cultura orientada a la

gestion del riesgo y control que debe permear todos los niveles organizacionales, lo que exige analizar e intervenir elementos básicos, en cuanto a la planeación estratégica institucional, la estructura organizacional, los procesos, la gestión del talento humano, recursos y bienes utilizados para la prestación del servicio, así como el conocimiento claro de los grupos de valor que atiende las diferentes entidades públicas. En este sentido, dentro del mismo capítulo se orienta sobre el desarrollo y mejora de la plataforma estratégica y los modelos de operación por procesos que pueden variar dependiendo de la complejidad y estructura de las entidades.

Como parte de este capítulo II, se explica y sustenta el análisis de niveles de madurez para la gestión del riesgo que permite establecer y comprender los componentes para su evaluación e intervención, para lo cual se incluye una herramienta de aplicación práctica; se explican de forma detallada los aspectos mínimos a incluir en la estructura de la política para la gestión integral del riesgo; se explica el marco conceptual sobre el apetito del riesgo, como referente para análisis, de acuerdo a la complejidad y naturaleza de las entidades que implementan y adoptan la presente guía.

De igual forma en este aparte, se precisa el esquema de articulación para los ámbitos o categorías de riesgos que se desagregan, que permitirán una gestión integral de riesgos, eje esencial para el desarrollo de los capítulos específicos sobre riesgos para la integridad pública, riesgos fiscales, riesgos de seguridad de la información y otros riesgos que se asocian a sectores regulados, como es el Sector Financiero y de Salud.

El capítulo III desarrolla los lineamientos y metodología aplicable para los Riesgos Generales de la Gestión, base para la identificación y valoración de las demás categorías de riesgos ya señalados, como elementos comunes para alcanzar la gestión integral de riesgos.

El capítulo IV precisa el manejo para una gestión preventiva de riesgos fiscales que permite a las entidades 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.

En el capítulo V, el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), como líder de la política de gobierno digital, define los lineamientos y metodologías aplicables para la gestión de riesgos de seguridad de la información, que permite incrementar la confianza de las partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades.

En el capítulo VI, la Secretaría de Transparencia de la Presidencia de la República, como líder de la política de Transparencia, Acceso a la Información y Lucha contra la Corrupción, desarrolla los lineamientos para la implementación del Sistema Integral de Gestión de Riesgos para la Integridad Pública (SIGRIP) que permite implementar los requerimientos para los Programas de Transparencia y Ética Pública (PTEP), específicamente en su componente programático 3 que define acciones específicas para la gestión del riesgo, que modifica y amplía el capítulo sobre riesgos de corrupción de versiones anteriores.

El capítulo VII se encuentra referenciada la articulación de la Gestión del Riesgo para entidades públicas vigiladas por la Superintendencia Nacional de Salud, cuyo detalle se incluirá a través de un anexo específico que se encuentra en proceso de elaboración en coordinación con el Ministerio de Salud y Protección Social y las Superintendencia, como instancia de vigilancia y control.

Por último, en el capítulo VIII se sientan las bases conceptuales para el diseño y seguimiento a los Indicadores Clave de Riesgo (*Key Risk Indicators – KRI* por sus siglas en inglés), los cuales surgen como una herramienta fundamental para la toma de decisiones informadas, al suministrar información sobre riesgos emergentes y potenciales, así como eventos o puntos desencadenantes por situaciones externas que pueden tener impacto sobre el logro de los objetivos de la organización.

En la caja de herramientas se ubican los siguientes documentos técnicos y herramientas parametrizadas para su adaptación y aplicación por parte de las entidades:

Anexo 1: Matriz mapa riesgos parametrizada: Se actualiza con las modificaciones metodológicas y de tipologías de riesgo incluidas en la presente guía.

Anexo 2: Glosario: desarrolla los términos y definiciones usados por tipología de riesgos y generales para aspectos comunes de la metodología.

Anexo 3: Catálogo indicativo de puntos de riesgo fiscal: Establece los puntos de riesgo fiscal, a partir de los procesos donde se genera gestión fiscal, como referente para la identificación, análisis y valoración de esta tipología de riesgos.

Anexo 4: Matriz estado de madurez de la gestión del riesgo parametrizada: Esquema que evalúa los componentes que integran una óptima gestión del riesgo a la luz del marco COSO-ERM.

Anexo 5: Matriz Riesgos de Seguridad de la Información: Desarrolla un ejemplo aplicable desde la identificación del activo hasta la valoración del riesgo.

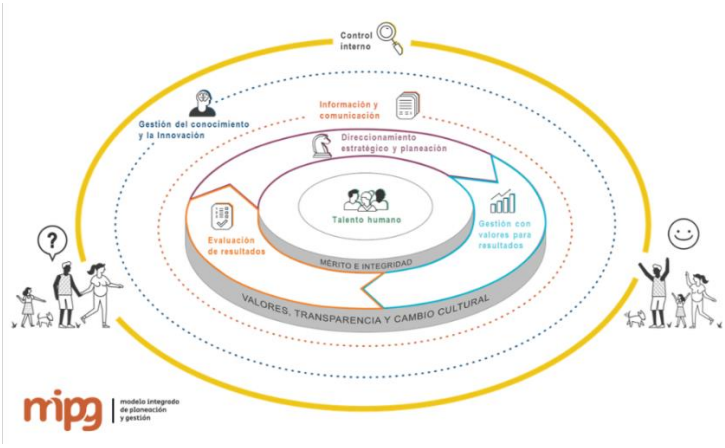
Capítulo I

Alineación estratégica de la Gestión del Riesgo y el Modelo Integrado de Planeación y Gestión MIPG

1.1 Articulación MIPG

El Modelo Integrado de Planeación y Gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio (Manual operativo MIPG, 2024, p. 9). El MIPG opera a través de 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y, finalmente, control interno) en las cuales se agrupan las políticas de gestión y desempeño institucional. Su implementación de manera articulada e interrelacionada, permite que el modelo funcione y opere adecuadamente. La Figura 1 ilustra las 7 dimensiones del modelo:

Figura 1 Esquema general del modelo integrado de planeación y gestión (MIPG)



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

Actualmente, el Modelo Integrado de Planeación y Gestión agrupa diecinueve (19) políticas, de las cuales es posible resaltar por lo menos diez (10) que tienen una relación directa con la administración de riesgos y el diseño de controles.

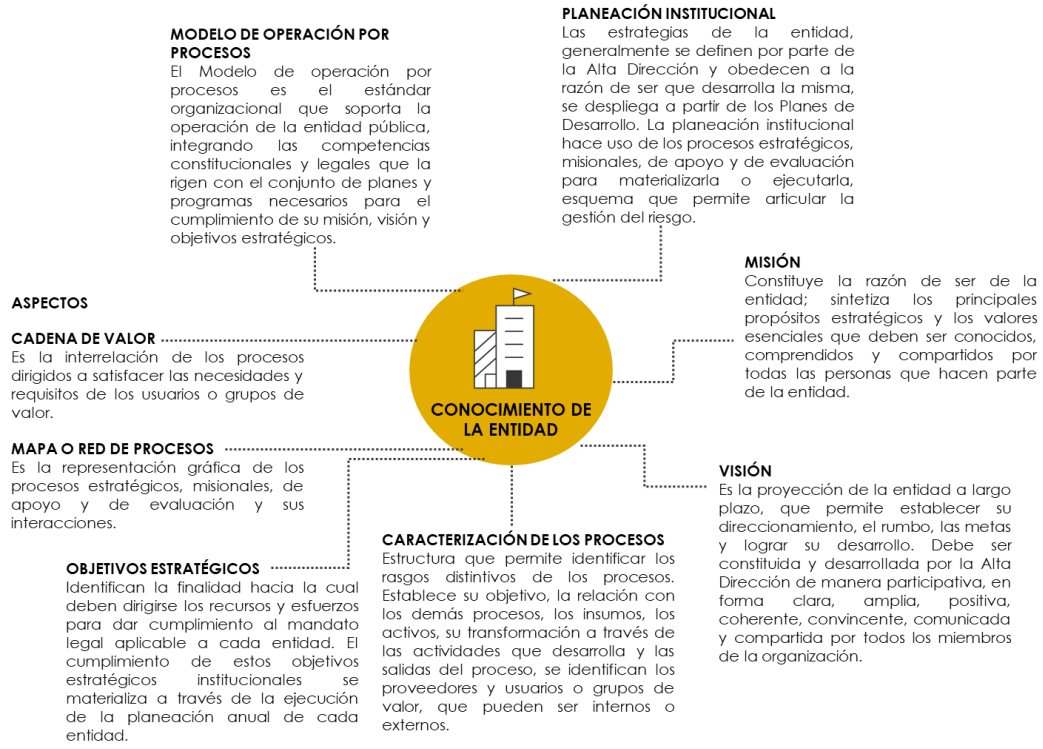
Desde la dimensión de Direccionamiento Estratégico se articulan con la gestión del riesgo las siguientes políticas:

- La **política de planeación institucional** busca que las entidades definan la ruta estratégica y operativa que guiará la gestión de la entidad, con miras a satisfacer las necesidades de sus grupos de valor. La implementación de la política de riesgo aporta al desarrollo de objetivos, estrategias y mecanismos para asegurar el logro de la misión o propósito fundamental para el cual fue creada la entidad, a partir del conocimiento de los derechos, necesidades y problemáticas de los grupos de valor a los cuales dirige sus productos o servicios y la consideración de las condiciones del entorno en el que se desempeña, los recursos con los que cuenta para establecer de manera coherente las metas y resultados esperados y en consecuencia, establecer los límites de desviación deseados y tolerables.

  El análisis de las capacidades organizacionales y de las condiciones del entorno permite examinar los factores que pueden afectar el logro de los objetivos y metas propuestas y con ello identificar los tratamientos apropiados para optimizar las medidas o tratamientos pertinentes para abordarlos. En este sentido, es claro que la definición de la política, así como la identificación de riesgos debe desarrollarse en el momento mismo en que es definida la estrategia, y los mismos, son parte del despliegue de los objetivos de la entidad, orientando así la toma de decisiones cotidiana en cada uno de los procesos, de tal forma que la definición, aprobación y comunicación de la estrategia, aporte también la información acerca de los riesgos que puede conllevar su desarrollo.

Este despliegue se da en los diferentes niveles de la organización, por lo que cada entidad, de acuerdo con su esquema de direccionamiento estratégico, procesos, procedimientos, políticas de operación y sistemas de información, tendrá insumos esenciales para iniciar con la aplicación de la metodología propuesta para la administración del riesgo. En la Figura 2 se puede observar esta interrelación.

Figura 2 Conocimiento y análisis de la entidad



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

- La **política de gestión presupuestal y eficiencia del gasto público** busca *que las entidades utilicen los recursos presupuestales de que disponen de manera apropiada y coherente con el logro de metas y objetivos institucionales, ejecutar su presupuesto de manera eficiente, austera y transparente y llevar un adecuado control y seguimiento*; del mismo modo, la **política de compras y contratación pública** permite *a las entidades*

estatales alinearse con las mejores prácticas en abastecimiento y contratación, para fortalecer la satisfacción de las necesidades públicas (eficacia), con optimización de recursos (eficiencia), altos estándares de calidad, pluralidad de oferentes y garantía de transparencia y rendición de cuentas.

Buena parte de la gestión fiscal se enmarca en la implementación conjunta de estas dos políticas, por lo tanto, se asocian a muchas de las actuaciones y decisiones que requieren la definición de controles para mitigar riesgos fiscales y riesgos contra la integridad pública. La programación y ejecución de los recursos, así como los procesos de adquisición de bienes y servicios no solo deben asegurar el cumplimiento de los requisitos normativos, técnicos y operativos, sino que deben orientarse al cumplimiento de los objetivos de la entidad y a la generación de valor público con criterio de eficiencia.

Así, en una gestión integral del riesgo, la aplicación y el desarrollo de estas políticas implican:

Desde la perspectiva de Gobernanza y Cultura:

- ✓ Incorporar **cultura de integridad y transparencia** en la administración de recursos.
- ✓ Exigir al Comité institucional de gestión y desempeño la supervisión activa del riesgo de los riesgos inherentes a la gestión presupuestal.

Desde la perspectiva de la definición de la Estrategia y el Establecimiento de Objetivos:

- ✓ Considerar en la articulación de la planeación estratégica con los **Planes de Desarrollo (nacionales o territoriales)** y los **Planes Operativos Anuales de Inversión,** el análisis de los riesgos presupuestales que puedan limitar o afectar su ejecución.
- ✓ Establecer objetivos presupuestales y financieros que apoyen el logro de los objetivos estratégicos previstos.

Desde la perspectiva de identificación y Evaluación de Riesgos:

- ✓ Realizar **mapas de riesgos** considerando los riesgos propios de la gestión presupuestal y de contratación.
- ✓ Evaluar el impacto de los riesgos en **eficiencia del gasto público** y el cumplimiento de la **regla fiscal**.
- ✓ Considerar análisis prospectivos (riesgos macroeconómicos, caída de ingresos tributarios, retrasos en transferencias, entre otros).

Desde la perspectiva de la respuesta al riesgo y la selección de Estrategias:

- ✓ Definir **controles internos presupuestales** basados en riesgos, no solo en procedimientos normativos.
- ✓ Implementar **alertas o indicadores claves** sobre sobre los riegos presupuestales y de contratación identificados.

Desde la perspectiva de información, comunicación y reporte:

- ✓ Publicar la información presupuestal, conforme la normativa vigente.
- ✓ Elaborar y comunicar informes de gestión que den cuenta de la **eficiencia y efectividad del gasto**, más allá del cumplimiento de las apropiaciones.
- ✓ Promover la comunicación abierta y oportuna con los diferentes grupos de valor y otras partes interesadas, respecto a los resultados de la gestión presupuestal y contractual (**rendición de cuentas**).

Desde la perspectiva de revisión y Monitoreo:

- ✓ Facilitar las auditorías internas y externas y propiciar en estas la cobertura de los riesgos presupuestales críticos.
- ✓ Incorporar **indicadores de desempeño y costo-eficiencia** en el ciclo presupuestal.
- ✓ Promover el uso de herramientas analíticas para detectar **alertas tempranas de corrupción o ineficiencia** en la gestión presupuestal y de contratación.

Desde la dimensión de Gestión con valores para resultados, la gestión del riesgo se relaciona con las siguientes políticas:

- La **política de fortalecimiento organizacional y simplificación de procesos** busca fortalecer las capacidades organizacionales mediante la alineación entre la estrategia institucional y el modelo de operación por procesos, la estructura y la planta de personal, de manera que contribuyan a optimizar procesos y trámites para los ciudadanos, mejorar la eficiencia administrativa y la calidad del servicio; para aportar un mayor valor público en la prestación de bienes y servicios, aumentando así la productividad estatal.

  La entidad define los procesos que sean necesarios para ordenar e interrelacionar las actividades requeridas para cumplir la misión y para generar los resultados propuestos de la planeación estratégica; en la identificación de cada uno de los procesos se establece el objetivo en función del aporte a la estrategia institucional, la secuencia de actividades requeridas, los responsables, los riesgos, los puntos de control y los indicadores claves para la medición de éstos.

  A partir del esquema de procesos, se definen procedimientos, políticas de operación, sistemas de información, manuales y otros instrumentos que permiten diseñar y establecer controles para gestionar de forma efectiva los riesgos que pueden afectar el cumplimiento de los objetivos, considerando incluso el aprovechamiento de estos cuando, constituyan oportunidades.

- La **política de servicio al ciudadano** tiene como propósito garantizar el acceso efectivo, oportuno y de calidad de los ciudadanos a sus derechos en todos los escenarios de relacionamiento con el Estado, Su cabal cumplimiento implica que las entidades orienten su gestión a la generación de valor público y de un Estado abierto que diseña e implementa soluciones a la medida de las necesidades, preferencias y

expectativas de la ciudadanía para la garantía de los derechos y el cumplimiento de obligaciones.

Una aplicación efectiva de las políticas de fortalecimiento organizacional y simplificación de procesos, así como de la de servicio al ciudadano, apoyada en la gestión de riesgos debería conducir a acciones tales como:

- ✓ La supervisión de los riesgos propios de los procesos de reorganización en instancia del Comité Institucional de Gestión y Desempeño.
- ✓ El desarrollo de estrategias para promover la gestión del cambio, como parte de una cultura de **control interno y mejora continua**, sólida.
- ✓ Considerar metas de simplificación de trámites y eficiencia en la planeación estratégica.
- ✓ Considerar y evaluar riesgos que puedan afectar la **continuidad del servicio al ciudadano**.
- ✓ Evaluar y documentar el análisis de riesgos requerido en procesos de cambio organizacional.
- ✓ Incorporar objetivos de eficiencia administrativa y simplificación de trámites en las actividades de auditoría y monitoreo planificadas.
- ✓ Establecer metodologías para implementar ajustes periódicos en los procesos, con fundamento en la retroalimentación ciudadana y la de los entes de control.

- La **política de seguridad digital** fortalece las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

La responsabilidad de las entidades públicas en la gestión de los datos de los ciudadanos y en general de sus grupos de valor conlleva la necesidad de asegurar la integridad, disponibilidad y confidencialidad de la información propia de su operación. Parte de este propósito se desarrolla a través de la identificación y clasificación de activos de información (pública, reservada, sensible), como parte de evaluación de riesgos de seguridad de la información y la aplicación de la **política de gestión Documental**; relacionadas también con la Dimensión de Información y Comunicación a través de la cual se concretan acciones de difusión, protección y conservación de los datos y la información institucional.

- La **política de transparencia, acceso a la información pública y lucha contra la corrupción** permite a la entidad articular acciones para la prevención, detección e investigación de los riesgos en los procesos de la gestión administrativa y misional de las entidades públicas, así como garantizar el ejercicio del derecho fundamental de acceder a la información pública a los ciudadanos y responderles de buena fe, de manera adecuada, veraz, oportuna y gratuita a sus solicitudes de acceso a la información pública.

  De conformidad con el Anexo técnico del Decreto 1122 de 2024, los Programas de Transparencia y Ética Pública – PTEP, se constituyen en el conjunto de acciones que una entidad define e implementa para promover, al interior de la organización, una cultura de la legalidad e identificar, medir, controlar y monitorear los riesgos de corrupción que se presentan en el desarrollo de su misionalidad herramientas para que las entidades públicas implementen acciones para promover la cultura de la legalidad, identificar, medir, controlar y monitorear los riesgos de corrupción.

  A su vez, el Programa de Transparencia y Ética Pública, en relación con el MIPG, vincula lineamientos de diferentes políticas de gestión y desempeño, con el fin de generar un esquema articulado para la prevención, detección y respuesta a situaciones

que afecten la transparencia y la ética pública, que pueden configurarse en diferentes ámbitos de la gestión institucional, lo que exige un análisis integral de los procesos que se desarrollan en las entidades.

Se trata entonces de vincular en el PTEP herramientas e instrumentos de gestión de riesgos ya desarrollados por políticas institucionales, para una gestión integral de prevención, detección y respuesta frente a riesgos de corrupción, fraude o soborno; de los conflictos de interés, los incumplimientos al código de integridad, riesgos fiscales, de lavado de activos y otros que puedan afectar la imagen y confianza institucional de cara a la ciudadanía.

Desde la dimensión de Talento Humano se resalta la política de integridad que vincula los lineamientos del Programa de Transparencia y Ética Pública.

- La **política de integridad** tiene como propósito institucionalizar la cultura de integridad como un proceso amplio y transversal al servicio público para garantizar el desempeño institucional responsable y el comportamiento probo de los servidores en función del interés general. Se busca con la implementación de esta política consolidar la gestión íntegra en el servicio público y el comportamiento ético de los servidores y contratistas en función de los intereses públicos, apoyados en la implementación del Código de Integridad y la gestión de conflictos de interés.

  La política de integridad debe desarrollarse a través de acciones concretas inmersas en los procesos de planeación estratégica, articulando acciones de gestión del talento humano, fomento de la cultura de autocontrol autogestión y auto regulación, así como de rendición de cuentas, para aportar así a la prevención de riesgos contra la integridad pública.

Las Dimensiones de Evaluación de Resultados y de Control Interno incorporan el monitoreo de riesgos y la evaluación de la efectividad de los controles desarrollados por los roles de primera, segunda y tercera línea, cada una de éstas en el ámbito de sus funciones:

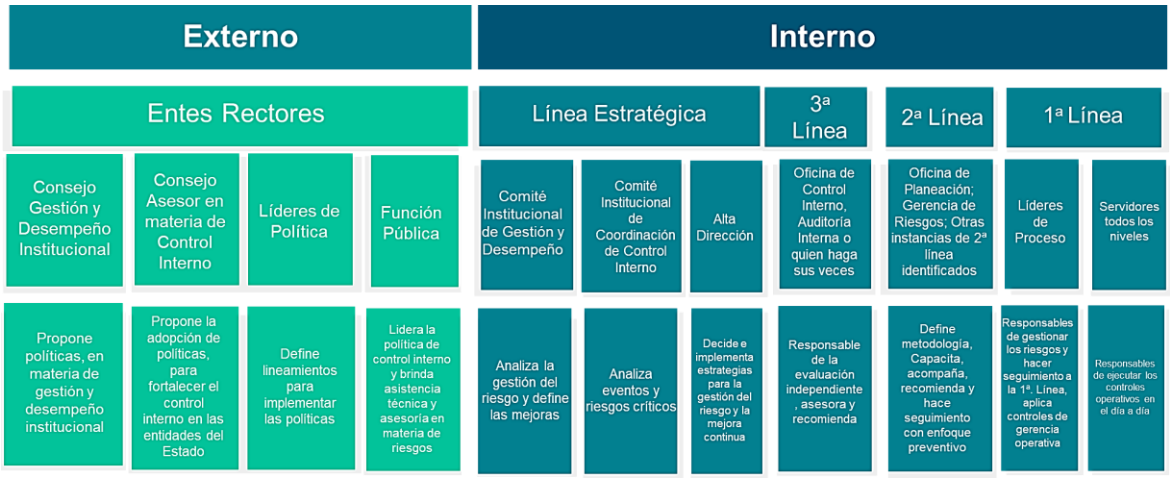
- En cumplimiento de la **política de seguimiento y evaluación del desempeño institucional**, a partir de la cadena de valor y la planeación estratégica, la entidad formula los indicadores que le permiten medir su gestión, ya sea como indicadores clave de proceso o indicadores clave de riesgo. El análisis de la medición de los indicadores permite generar las alertas, ajustar los controles y tomar las decisiones para conducir las acciones hacia el logro de los objetivos.

- La promoción de las **políticas de control interno**, como base fundamental de un adecuado ambiente y tono de control en las entidades, es uno de los principales roles de la Alta dirección, el Comité Institucional de gestión y el desempeño y el Comité Institucional de Coordinación de Control Interno. Estas políticas se desarrollan a través de los diferentes componentes y elementos del Modelo Estándar de Control Interno – MECI, y su propósito fundamental es que el sistema de control interno y de gestión, apoyen con efectividad el logro de los objetivos estratégicos y misionales de cada entidad.

1.2 Institucionalidad

El Modelo Integrado de Planeación y Gestión define para su operación instancias que trabajan coordinadamente para que el Modelo funcione adecuadamente; desde la perspectiva de Gestión del Riesgo pueden resumirse como lo ilustra la figura 3:

Figura 3 Institucionalidad del MIPG desde la perspectiva de Gestión de Riesgo



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

Nota: En entidades de alta complejidad se puede considerar la figura de gestores de riesgos. Se trata de personas clave en las áreas o procesos que ayudan al líder de proceso y a la 2ª línea de defensa en la gestión del riesgo, esta figura es opcional no obligatoria en su implementación.

Tanto el Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017 son instancias de alto nivel al interior de las entidades que orientan la toma de decisiones estratégicas para la operación del Modelo, la gestión efectiva de los riesgos que puedan afectar la consecución de los objetivos institucionales y fomentan la adhesión a los valores, las políticas, las disposiciones normativas aplicables, los procesos y controles establecidos por la entidad y que componen en su conjunto todos los instrumentos y mecanismos de gestión del Modelo.

El Comité Institucional de Gestión y Desempeño se encarga de orientar la implementación y operación del MIPG y para ello, cumple entre otras funciones las siguientes que impactan la gestión de riesgos:

- ✓ Aprobar y hacer seguimiento a las acciones y estrategias adoptadas para la operación del MIPG, lo que implica entre otros, aprobar la política de gestión de riegos de la entidad y propiciar su actualización periódica.
- ✓ Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del MIPG, lo que conlleva también, incorporar dentro de la planeación estratégica el análisis de riesgos para decidir respecto de los objetivos, las metas y niveles de riesgo aceptados y no aceptados en su consecución.
- ✓ Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión, lo que requiere establecer los mecanismos y responsables de monitorear el desempeño los resultados de la gestión de riesgos y compartir en dicha instancia estos resultados para la definición de las acciones estratégicas y/o o de mejora, consecuentes.

El Comité Institucional de Coordinación de Control Interno como órgano asesor e instancia decisoria en asuntos de control interno aporta a la gestión de riesgos mediante las siguientes funciones:

- ✓ Evaluar el estado del Sistema de Control Interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del sistema.
- ✓ Aprobar el Plan Anual de Auditoría de la entidad, hacer sugerencias y seguimiento a las recomendaciones, con el fin de asegurar que su alcance y recursos faciliten la cobertura de los proyectos estratégicos de la entidad, así como la priorización de los las unidades auditables críticas para la misma, según la priorización y el análisis de riesgos hecho por la Oficina de Control Interno y/o quien haga sus veces.
- ✓ Servir de instancia para resolver las diferencias que surjan en desarrollo del ejercicio de auditoría interna.
- ✓ Conocer y resolver los conflictos de interés que afecten la independencia de la auditoría.

- ✓ 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.
- ✓ Verificar que el esquema de líneas atiende de manera íntegra la gestión del riesgo al interior de la entidad, comprometiendo todos los niveles de la organización.

1.3 La gestión de riesgos como pilar de buen gobierno y control institucional:

En el marco de la modernización del Estado Colombiano y la implementación de un enfoque basado en resultados, la gestión de riesgos se consolida como una herramienta fundamental para fortalecer la toma de decisiones públicas, la transparencia, la eficacia institucional y la confianza ciudadana. Más allá de su función preventiva, la gestión de riesgos permite anticipar escenarios adversos, gestionar oportunidades y alinear la operación institucional con los objetivos estratégicos del Estado.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha señalado que los gobiernos deben adoptar una cultura de gestión de riesgos que permita garantizar la resiliencia institucional, la integridad de las políticas públicas y la protección de los recursos públicos frente a incertidumbres, presiones sociales, tecnológicas o fiscales (OCDE, *Framework for the Governance of Critical Risks*, 2014). En este sentido, se reconoce que los riesgos no solo deben gestionarse a nivel operativo, sino que requieren de un compromiso institucional desde el más alto nivel directivo.

1.4 Gobernanza, tono desde la cima y gestión de riesgos:

Una gestión de riesgos efectiva en el sector público parte de un elemento esencial: el tono de control que establecen los órganos de dirección, representación legal y alta gerencia, quienes deben asumir el liderazgo en la promoción de una cultura organizacional consciente del riesgo, ética, proactiva y orientada a la integridad. Esta postura implica no solo emitir directrices, sino incorporar la gestión de riesgos en los procesos de planeación, ejecución y seguimiento institucional.

El concepto de “gobernanza del riesgo” hace referencia a los arreglos institucionales y de control que aseguran que los riesgos sean conocidos, comunicados, gestionados y monitoreados en toda la entidad. La OCDE plantea que una adecuada gobernanza del riesgo requiere:

- ✓ Liderazgo claro y responsabilidad de la alta dirección.
- ✓ Marcos normativos y estructuras institucionales apropiadas.
- ✓ Evaluación y priorización de riesgos basada en evidencia.
- ✓ Coordinación interinstitucional y comunicación transparente.

En el contexto colombiano, el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo Estándar de Control Interno (MECI), ambos adoptados mediante el Decreto 1499 de 2017 y el Decreto 1083 de 2015 (modificado), establecen que la gestión de riesgos es un componente transversal de los sistemas de gestión pública. El dominio de control del MECI enfatiza la importancia del “Ambiente de Control”, dentro del cual el tono desde la cima representa la base para la implementación efectiva del control interno, incluyendo la prevención del fraude, la corrupción y otras prácticas indebidas.

1.5 Beneficios de una adecuada gestión integral del riesgo en la administración pública:

Adoptar un enfoque sistemático de gestión de riesgos en el sector público implica:

- ✓ Reconocer la incertidumbre inherente a la formulación e implementación de políticas públicas.
- ✓ Identificar amenazas y oportunidades que puedan afectar los objetivos misionales y estratégicos.
- ✓ Proteger los recursos públicos y fortalecer la rendición de cuentas ante la ciudadanía y los órganos de control.

- ✓ Alinear la gestión institucional con principios de buen gobierno, legalidad, eficiencia y transparencia.

En este sentido, la gestión de riesgos no es un ejercicio accesorio o de cumplimiento formal. Es un componente central de la gobernanza pública moderna, que contribuye al logro de resultados sostenibles y al fortalecimiento de la democracia administrativa.

En este sentido, entre los beneficios de la gestión integral del riesgo para la entidad, se identifican los siguientes:

- ✓ **Incrementa la capacidad de la entidad para alcanzar sus objetivos:** El foco de todas las etapas de la gestión del riesgo es alinear las políticas y prácticas de operación frente a los objetivos estratégicos de la entidad, por tanto, todas las acciones de gestión y control se orientan a asegurar su cumplimiento, lo cual se traduce en la generación de productos y servicios pertinentes, oportunos y de calidad dirigidos a satisfacer las necesidades de los grupos de valor. La toma de decisiones que se apoya una debida evaluación de riesgos, análisis de controles y recursos disponibles, resulta más eficaz, eficiente y oportuna ya que permite anticiparse a situaciones internas o externas que pueden afectar o potencializar los resultados deseados

- ✓ **Fomenta la continuidad del servicio y/o la operación normal de la organización:** El hecho de minimizar la probabilidad e impacto de los riesgos proporciona estabilidad y permite enfocar los esfuerzos al mejoramiento en la calidad de los procesos y en consecuencia a mejorar los resultados. La gestión integral del riesgo dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente.

- ✓ **Fortalecimiento de la cultura de riesgos y control de la organización:** Involucrar a todos los servidores como responsables de la gestión de los riesgos les concientiza sobre la interacción de los procesos, la orientación estratégica, el uso racional de los recursos y la agregación de valor, lo cual aporta a la consolidación de un servicio público

orientado al desarrollo efectivo de su misión y al desarrollo de acciones estratégicas y de mejora continuas, para alcanzar su visión, en ambos casos en un ámbito de integridad y transparencia.

Capítulo II

Aspectos clave antes de aplicar la metodología

La gestión integral de riesgos, es posible definirla como "*la cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo, de cara la creación, preservación y materialización de valor*." (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.10). Esta definición, adoptada en esta guía, implica que la gestión del riesgo se consolida a través de: i) el reconocimiento de la cultura; ii) el desarrollo de capacidades; iii) el uso de las técnicas aplicadas; iv) la integración de la estrategia y el desempeño; v) la alineación con la estrategia y objetivos clave y vi) la relación con el valor.

El reconocimiento de la cultura, como base fundamental de un sistema de gestión y de control interno efectivo, implica reconocer que son las personas quienes la desarrollan y dan forma a la misma en todos los niveles, a través de sus comportamientos y toma de decisiones, por lo que, cimentar desde la Alta dirección una sólida cultura de riesgos y un tono apropiado de control, es determinante para propiciar la evaluación y valoración de riesgos de forma intrínseca en todo proceso de toma de decisiones. Reconocer el efecto de la cultura en la gestión institucional, implica también reconocer la importancia de desarrollar de forma continua estrategias o actividades orientadas a fortalecerla continuamente para apalancar con mayor éxito el logro de los objetivos.

La gestión del riesgo promueve el desarrollo de capacidades que permiten a las entidades identificar, prever y enfrentar los desafíos de su entorno, para adaptarse al cambio y estar en mejores condiciones de mejorar continuamente su gestión.

La aplicación de técnicas es un proceso dinámico que requiere desarrollarse de forma continua frente a todas las actividades e iniciativas con impacto en los objetivos estratégicos y en todos los niveles de la entidad, con el objetivo de que todas las personas de la entidad

comprendan en la cotidianidad de sus actividades, cuál es la estrategia institucional, cuáles los objetivos, los riesgos y los niveles aceptados de riesgo; lo que facilita la toma de decisiones y la gestión adecuada de los recursos bajo su responsabilidad.

Para la integración de la estrategia y el desempeño, es clave comprender la forma como dicha estrategia apalanca la misión y visión, y cómo se despliega hacia los objetivos de los procesos, programas y proyectos a cargo de la entidad, donde la gestión del riesgo es crucial para determinar en diferentes ámbitos organizacionales: los tipos de riesgos a los cuales se enfrenta, reconocer y monitorear los indicadores claves de desempeño y actuar conforme a sus resultados, para avanzar de forma continua y proactiva en la generación de un valor público que deriva de la satisfacción de las necesidades y expectativas de los diferentes grupos de interés.

En este marco general, será imprescindible que se consideren elementos básicos en cuanto a la planeación estratégica institucional, la estructura organizacional, los procesos, la gestión del talento humano, recursos y bienes utilizados para la prestación del servicio, así como el conocimiento claro de los grupos de valor que atiende las entidades públicas objeto de la presente guía.

2.1 Análisis Estratégico de la entidad y su modelo de Operación basada en procesos:

Para el análisis estratégico de la entidad es necesario que el Modelo Integrado de Planeación y Gestión (MIPG) sea visto de manera integral, dado que las políticas y dimensiones que lo integran se articulan de manera directa con una adecuada gestión por procesos. En particular, la dimensión de Direccionamiento Estratégico contempla que una entidad debe realizar un análisis del entorno tanto específico como general, así como un análisis de capacidades internas.

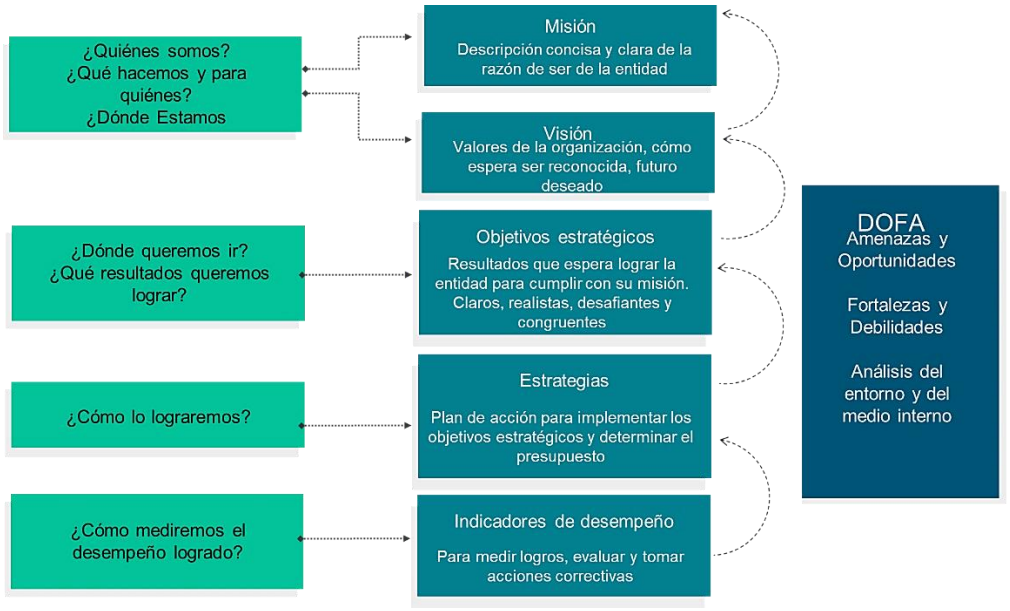
La gestión por procesos se constituye en el eslabón que conecta la planeación estratégica de cualquier entidad con el despliegue de la parte operativa. Para ello, toma como insumos

algunos elementos de la dimensión de direccionamiento estratégico en la medida en que debe alinearse con la misión, visión y objetivos estratégicos, entre otros.

La planeación estratégica en el ámbito público es un instrumento que ayuda al establecimiento de prioridades, objetivos y estrategias como apoyo a la definición de los recursos que se requieren para lograr los resultados esperados. (Amijo, 2011).

A continuación, en la figura 4 se desarrolla un modelo básico de planeación estratégica, donde se precisan las preguntas que pueden orientar la construcción de cada uno de los componentes:

Figura 4 Modelo básico de planeación estratégica



Fuente: adaptado de CEPAL, Serie Manuales N° 69, Planificación estratégica e indicadores de desempeño en el sector público. Amijo, Marinela, Chile, junio de 2021.

Para mayor detalle sobre la gestión por procesos, se recomienda consultar la Guía para la gestión por procesos en el marco MIPG[3], la cual se encuentra publicada en la caja de herramientas de la dimensión 7 de Control Interno, en el micrositio de MIPG, alojado en nuestra página Web.

En atención a lo antes referido, la entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desarrollo hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características SMART, cuya estructura se explica a continuación en la figura 5:

Figura 5 Desglose características SMART para redacción Objetivos

Fuente: Adaptado por Dirección de Gestión y Desempeño Institucional de Función Pública, 2025, de acuerdo con: https://www.questionpro.com

2.2 Niveles de Madurez para la Gestión del Riesgo:

Teniendo en cuenta que la gestión estratégica del riesgo involucra una serie componentes y elementos que se deben fortalecer desde la cultura organizacional, se hace necesario evaluar su nivel de madurez. Para este efecto, atendiendo uno de los marcos que sustentan

[3] Guía para la gestión por procesos en el marco del modelo integrado de planeación y gestión (Mipg) - Versión 1 - Julio de 2020 - https://www1.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/36963907

el desarrollo de la presente guía que corresponde al COSO-ERM-2017 se propone una estructura que, "*consta de cinco componentes interrelacionados de la gestión del riesgo empresarial y su relación con la misión, visión y valores clave de la entidad*". Gráficamente se observan "*tres cintas que muestran el Establecimiento de Estrategias y de los Objetivos, Desempeño, Revisión y Monitorización representan los procesos más habituales que fluyen a través de la entidad. Las otras dos cintas de, Gobierno y cultura, e Información, Comunicación y Reporte, representan aspectos de apoyo a la gestión del riesgo empresarial*". (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.11). Esta estructura se puede observar en la figura 6.

Figura 6 Estructura COSO-ERM

Fuente: IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017

Los cinco componentes que integran una óptima gestión del riesgo a la luz de este marco de referencia, se describen a continuación:

Gobierno y Cultura: El gobierno y cultura juntos forman una base para todos los demás componentes de la gestión del riesgo empresarial. El gobierno marca el tono

de la entidad, reforzando la importancia de la gestión del riesgo empresarial y estableciendo responsabilidades de supervisión al respecto. La cultura se refleja en la toma de decisiones.

Establecimiento de la estrategia y objetivos: La gestión del riesgo empresarial se integra en el plan estratégico de la entidad a través del proceso de establecimiento de la estrategia y de los objetivos de negocio. Con un conocimiento profundo del contexto empresarial, la organización puede comprender mejor los factores internos y externos y sus efectos en el riesgo. (…)

Desempeño: Una organización identifica y evalúa los riesgos que pueden afectar la capacidad de una entidad para alcanzar la estrategia y los objetivos de negocio. (…). La organización entonces selecciona las respuestas al riesgo y efectúa seguimiento del desempeño considerando posibles cambios.

Revisión y monitorización: Al examinar las capacidades y técnicas de gestión del riesgo empresarial, y el desempeño de la entidad en relación con sus objetivos. (…)

Información, Comunicación y Reporte: La comunicación es el proceso continuo e iterativo de obtener y compartir información en toda la entidad. La Dirección utiliza información pertinente de fuentes internas y externas para facilitar la gestión del riesgo empresarial. La organización aprovecha los sistemas de información para capturar, procesar y gestionar datos e información. Al utilizar información que se aplica a todos los componentes, la organización informa sobre el riesgo, la cultura y el desempeño. (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.11, 12).

Bajo este marco, para el análisis de niveles de madurez se propone un esquema de diagnóstico que analiza los componentes y principios que desarrolla el modelo COSO-ERM, a partir de una serie cuestiones o puntos de reflexión que se responden asignando una calificación de 1 a 5 para cada uno de los principios por componente que se describen en la tabla 1:

Tabla 1 Componentes y principios evaluables modelo de madurez

Componente	Principios
Gobierno y Cultura	Supervisión de riesgos a través del consejo de administración.
	Establece estructuras operativas
	Define la cultura deseada
	Demuestra compromiso con valores clave
	Atrae, desarrolla y retiene a profesionales capacitados
Establecimiento de la estrategia y objetivos	Analiza el contexto (externo e interno)
	Define el apetito del riesgo
	Evalúa estrategias alternativas
	Formula objetivos estratégicos y operacionales
Desempeño	Identifica y describe el riesgo
	Evalúa el riesgo inherente
	Diseña controles efectivos
	Prioriza riesgos
	Desarrolla visión integral
Análisis y monitorización	Evalúa los cambios significativos
	Revisa el riesgo y el desempeño
	Persigue la mejora de la gestión del riesgo
Información, Comunicación y Reporte	Aprovecha la información y la tecnología
	Comunica información sobre riesgos
	Informa sobre el riesgo, la cultura y el desempeño

Fuente: Adaptado por Dirección de Gestión y Desempeño Institucional a partir de Auditoría Interna y gestión de riesgos, Instituto de Auditores de España. Octubre 2021

Una vez calificados los principios por cada uno de los componentes, a partir de los puntos de reflexión que se plantean en la herramienta propuesta con un esquema de preguntas orientadoras, se establecerá el grado de madurez para la gestión del riesgo en el que se ubica la entidad. El instrumento propuesto consolida o resume los resultados por componente y genera un mapa de calor, donde se resaltarán los temas a intervenir en una escala de severidad o prioridad para su atención, de tal manera que las Oficinas de Planeación o gerencias de riesgos, como instancias de 2ª línea, puedan proponer a la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno u otra instancia del mismo nivel jerárquico las orientaciones o acciones que desde allí deben surgir para garantizar la gestión integral del riesgo en la entidad.

Para efectos de la calificación de cada principio, la entidad deberá establecer el grado en que cada uno de estos se encuentra implementado (establecido en alguna política, proceso o directriz institucional), presente (práctica que es reconocida y aplicada de forma consistente) y operando de forma integrada (medida en que estas prácticas o políticas son reconocidas y aplicadas en todos los niveles de responsabilidad y procesos de la entidad.

Nota: Para aplicar el análisis sobre niveles de madurez como anexo en la caja de herramientas se ubica la ***Herramienta diagnóstico modelo de madurez.***

2.3 Política para la gestión integral de riesgos:

Para la elaboración de una política orientada a la gestión integral del riesgo, teniendo como referente el estándar ISO31000:2018 que desarrolla los principios y directrices de la gestión del riesgo, segundo marco base de la presente guía, dicho estándar en el numeral 5.2 señala:

> "***5.2 Liderazgo y Compromiso***
>
> *La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización y deberían demostrar el liderazgo y compromiso:*
>
> - *adaptando e implementando todos los componentes del marco de referencia;*
> - *publicando una declaración o una política que establezca un enfoque, un plan o una línea de acción para la gestión del riesgo:*
> - *asegurando que los recursos necesarios se asignan para gestionar los riesgos;*
> - *asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la organización.* (…)" (ISO31000:2018, p.5).

Bajo estas directrices, la Alta Dirección de las organizaciones debe asegurar que la gestión del riesgo se vincule a todas las actividades de la operación, para lo cual debe definir una política que establezca las líneas de acción o enfoque para la gestión del riesgo que incluya, la adopción de un marco de referencia, la disposición de recursos necesarios y la asignación de responsabilidades en los niveles adecuados, atendiendo la autoridad y responsabilidad, con el fin de hacer seguimiento y monitoreo integral a los riesgos.

Por su parte, en el marco del Modelo Integrado de Planeación y Gestión MIPG, desde la dimensión de Direccionamiento Estratégico y Planeación se establece:

> "*Esta es una tarea propia del equipo directivo y se debe hacer desde el ejercicio de Direccionamiento Estratégico y de Planeación. En este punto, se deben emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales* (…)" (Función Pública, Manual Operativo MIPG v6, 2024, p.36)

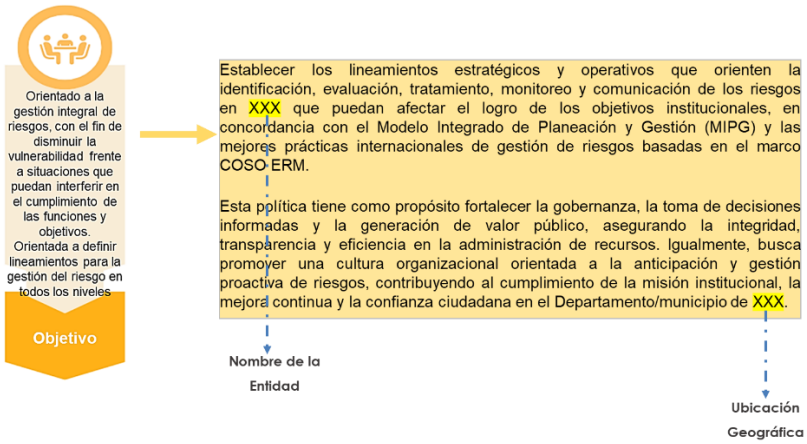
De acuerdo con las anteriores bases conceptuales, para la elaboración de la política para la gestión integral de riesgos se debe considerar que: i) para su formulación se requiere del compromiso y responsabilidad por parte de la Alta Dirección (Línea Estratégica); ii) debe aportar al como propósito fundamental de lograr los objetivos estratégicos de la entidad; iii) debe partir del análisis del contexto interno y externo, así como de la consideración de riesgos emergentes, para a partir de este análisis, prever la asignación de recursos y medidas consecuentes iv) debe definir los niveles de autoridad y responsabilidad frente al manejo de los riesgos, con el fin de garantizar su eficiencia en la implementación y efectividad para evitar afectaciones por materializaciones del riesgo que impidan el logro de los objetivos y metas institucionales y el buen uso de los recursos públicos.

En este sentido, la política para la gestión integral de riesgos puede estructurarse mediante instructivos o manuales internos, con el fin de poder desplegar una serie de elementos que son claves para la implementación de riesgos en todos los niveles organizacionales y para

su posterior seguimiento y monitoreo, en el marco del Esquema de Líneas, eje articulador de la política de control interno que desarrolla MIPG. Es importante que este documento incluya mínimo los siguientes aspectos, que a continuación se explican.

2.3.1 Objetivo de la política: Orientado a la gestión integral de riesgos, cuyo propósito es disminuir la vulnerabilidad frente a situaciones que puedan interferir en el cumplimiento de las funciones y objetivos de la entidad. Debe definir lineamientos para la gestión del riesgo en todos los niveles. La figura 7 muestra un ejemplo orientador.

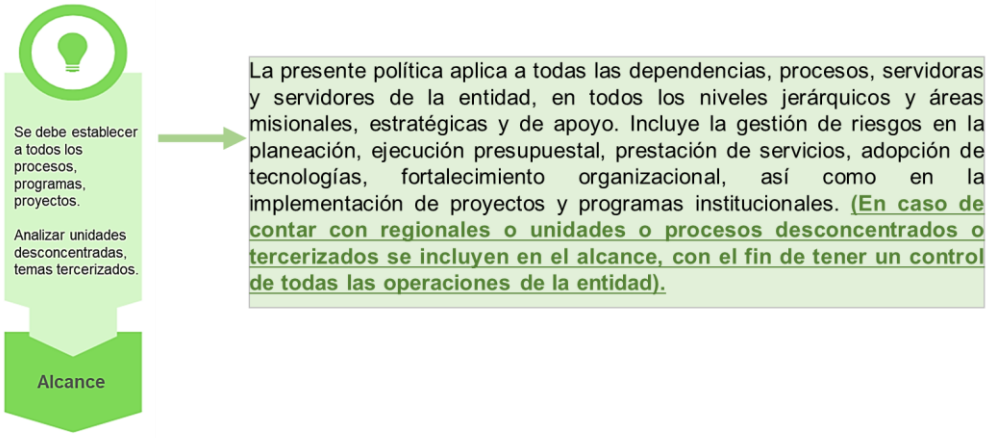
Figura 7 Ejemplo objetivo de la política



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional a partir lineamientos COSO-ERM. 2025

2.3.2 Alcance de la política: Debe dar cobertura a todos los procesos, programas y proyectos. De acuerdo a la naturaleza y misionalidad de cada entidad, será necesario analizar dentro del alcance unidades desconcentradas o temas tercerizados, operados por privados u otras entidades públicas a través de convenios, con el fin de establecer acciones de seguimiento, dado que estas organizaciones que son externas a la entidad pueden generar riesgos críticos que deben considerarse para su control. La figura 8 muestra un ejemplo orientador.

Figura 8 Ejemplo alcance de la política



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

2.3.3 Contexto Interno y externo: Es necesario desplegar un análisis interno y externo específico para la entidad, donde se expliquen mediante información institucional formalizada y datos específicos relacionados, teniendo en cuenta los siguientes elementos:

- ✓ **Contexto Interno**: estructura organizacional, cultura institucional, capacidad tecnológica, talento humano, procesos internos, recursos financieros, políticas internas y marco normativo aplicable.
- ✓ **Contexto Externo**: entorno político, económico, social, ambiental y tecnológico; actores del sector, reguladores, organismos de control, ciudadanos y partes interesadas, así como riesgos asociados a cambios normativos y eventos externos. Sector donde opera la entidad y su relacionamiento con otras entidades e instancias necesarias para su gestión, así como entorno de desarrollo territorial.

La figura 9 muestra un ejemplo orientador.

Figura 9 Análisis de contexto interno y externo

Contexto Externo	Contexto Interno
Despliegue problemáticas del sector o del territorio donde desarrolla las funciones la entidad.	Despliegue plataforma estratégica de la entidad (misión, visión, objetivos estratégicos). Estructura Organizacional.
Incluya datos de la población (No. Habitantes en zona urbana y rural); características de la región: datos económicos, sociales, de seguridad y orden de público.	Esquema de Operación por procesos, despliegue a políticas, procedimientos, sistemas de información y otros sistemas de gestión articulados (SST, SGC, Sistema Gestión Ambiental u otros aplicables). Infraestructura tecnológica.
Zonas de influencia (municipios cercanos, cercanía a zonas de frontera internacional).	Caracterización de grupos de Valor, Ciudadanos o Usuarios.

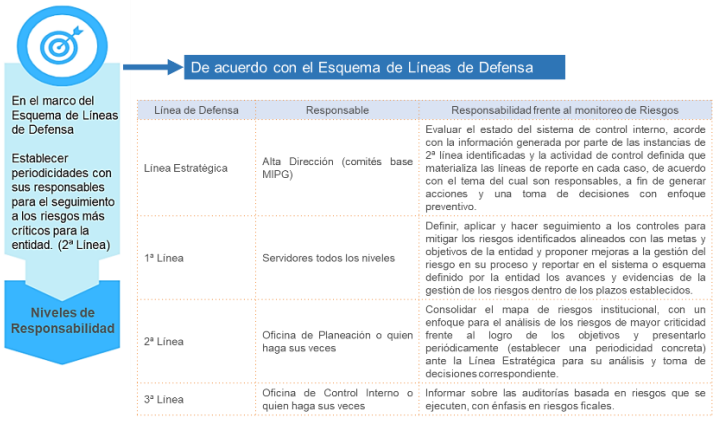
Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

2.3.4 Niveles de responsabilidad: En el marco del Esquema de Líneas, establecer las periodicidades con sus responsables para el seguimiento a los riesgos estratégicos y claves de la entidad, considerando con especial relevancia las responsabilidades de la Línea estratégica y Alta Dirección en términos de la definición del apetito de riesgo, la aprobación de la política y la asignación de recursos y responsabilidades para su implementación. Las de la primera línea o líderes de proceso, responsables de identificar, evaluar y controlar riesgos en sus diferentes procesos, proyectos o iniciativas estratégicas, dentro de estas las propias de todos los Servidores, responsables de reportar oportunamente los riesgos materializados, aplicar los controles establecidos y proponer proactivamente mejoras en los mismos cuando sean necesarias.

Las de la Oficina de Control Interno, en cuanto a la evaluación de la efectividad de los controles y la proposición de mejoras para hacer más efectiva la gestión de los diferentes tipos de riesgos

La figura 10 muestra un ejemplo.

figura 10 Niveles de responsabilidad para la gestión del riesgo



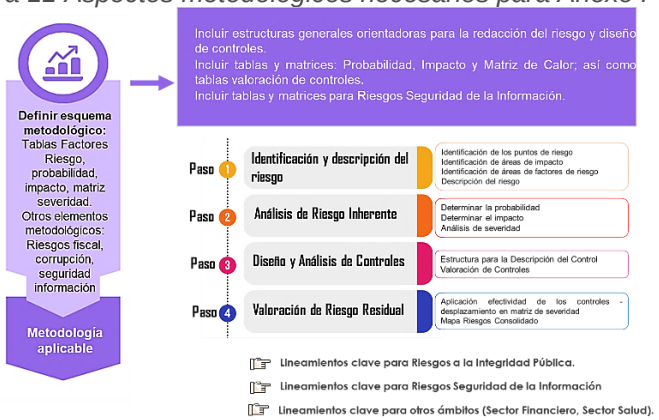
Línea de Defensa	Responsable	Responsabilidad frente al monitoreo de Riesgos
Línea Estratégica	Alta Dirección (comités base MIPG)	Evaluar el estado del sistema de control interno, acorde con la información generada por parte de las instancias de 2ª línea identificadas y la actividad de control definida que materializa las líneas de reporte en cada caso, de acuerdo con el tema del cual son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo.
1ª Línea	Servidores todos los niveles	Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso y reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
2ª Línea	Oficina de Planeación o quien haga sus veces	Consolidar el mapa de riesgos institucional, con un enfoque para el análisis de los riesgos de mayor criticidad frente al logro de los objetivos y presentarlo periódicamente (establecer una periodicidad concreta) ante la Línea Estratégica para su análisis y toma de decisiones correspondiente.
3ª Línea	Oficina de Control Interno o quien haga sus veces	Informar sobre las auditorías basada en riesgos que se ejecuten, con énfasis en riesgos fiscales.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

2.3.5 Definir el esquema metodológico aplicable: Como anexo a la política será necesario desplegar una estructura metodológica tomando como referencia la dispuesta en la presente guía, considerando elementos básicos como i) tabla factores de riesgo; ii) tablas de probabilidad e impacto; iii) matriz de severidad; iv) tabla valoración controles. Así mismo, incluir lineamientos clave para los riesgos a la Integridad Pública, riesgos fiscales y riesgos de seguridad de información, así como otros marcos y normatividad aplicable, dependiendo del sector al cual pertenece la entidad, especialmente aquellos requerimientos definidos por las instancias de vigilancia como las Superintendencias de Salud, Financiera, de Servicios Públicos Domiciliarios y otras, dependiendo de la naturaleza y funciones que desarrolla cada entidad, de manera tal que se cuente con toda información necesaria para la identificación, análisis y valoración de riesgos, con un enfoque integral.

Este anexo a la política, será objeto de actualización en la medida en que los marcos que sustentan la presente guía se actualicen o modifiquen, así como los cambios que pueden presentarse en sectores regulados y vigilados. En caso de que la entidad haya dispuesto un software o herramienta para su desarrollo, deberá explicarse su manejo. La figura 11 muestra estos aspectos clave.

Figura 11 Aspectos metodológicos necesarios para Anexo Política



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

NOTA: *Como parte de la caja de herramientas se incluye una estructura tipo de política que podrá ser adaptada, de acuerdo a la complejidad y necesidades de cada entidad.*

2.4 Marco conceptual sobre el apetito del riesgo: Teniendo en cuenta que, la política para la gestión integral del riesgo debe establecer el apetito del riesgo, es necesario precisar su aplicación, para lo cual, a continuación se definen los aspectos clave necesarios para su análisis, los cuales, en todo caso dependerán de la complejidad de cada entidad y su decisión corresponderá a la Alta Dirección o Línea Estratégica en el marco del Comité Institucional de Coordinación de Control Interno, Comité de Auditoría u otra instancia de este mismo nivel jerárquico.

Para poder iniciar con el análisis del apetito de riesgo, es necesario comprender la misión, visión, objetivos y estrategias, ya que este despliegue de la plataforma estratégica permite tener una perspectiva sobre el tipo y nivel de riesgo que es probable que enfrente la entidad.

En este marco general, cada entidad debe comprender la relación entre el riesgo y el desempeño, ya que a partir de los resultados alcanzados es posible obtener información valiosa para la definición del apetito del riesgo, dado que, "*al observar el desempeño actual, se puede identificar cómo las tendencias, relaciones y otros factores actuales están afectando el perfil de riesgo*". (COSO-ERM, 2017, p.48).

En cuanto a los parámetros a utilizar para su definición, cada entidad puede considerar análisis cualitativos y cuantitativos, lo cual dependerá de la naturaleza, funciones y sector donde desarrolla sus operaciones. Se debe tener en cuenta que:

> "*En las declaraciones cualitativas se describen los riesgos específicos de la organización que está dispuesta a aceptar; en las declaraciones cuantitativas, se describen los límites, umbrales o indicadores clave de riesgo, que establecen cómo han de ser juzgados los riesgos y sus beneficios y/o cómo evaluar y vigilar el impacto agregado de estos riesgos. Asimismo, es importante considerar aquellos elementos del apetito de riesgo que no se pueden medir y que, por tanto, podrían ser más difíciles de gestionar, como los riesgos reputacionales.* (…) *Todo ello se debe hacer de manera integral y equilibrada, de forma que las medidas cuantitativas se combinen con las medidas cualitativas, así como aquellos riesgos para los que la institución puede tener tolerancia cero, en esta tipología se encuentran aquellos riesgos relacionados con incumplimientos legales o regulatorios, riesgos relacionados con la seguridad de los empleados, riesgos de fuerte impacto medioambiental, etc*." (Instituto de Auditores de España, IIA Global, 2013).

Es relevante señalar que, la metodología de cálculo para determinar el apetito del riesgo puede estar condicionada por el sector donde desarrolla sus actividades, por lo que resulta relevante considerar las particularidades dependiendo si se opera en un mercado regulado, donde las entidades y empresas utilizan medidas cuantitativas para expresar su apetito del riesgo, mientras que para aquellas entidades que operan en otros sectores pueden optar por evaluaciones cualitativas o cuantitativas, o bien una combinación de ambas.

Al respecto, el Instituto de Auditores IIA Global en el análisis realizado sobre las perspectivas y percepciones globales en materia de gobernanza, riesgo y control, plantea para el análisis de apetito del riesgo lo siguiente:

> **El Marco Internacional de Práctica Profesional del IIA The IIA's** define el apetito de riesgo simplemente como "El nivel de riesgo que una organización está dispuesta a aceptar". En la práctica, el apetito de riesgo, también referido como tolerancia al riesgo, representa un equilibrio entre los beneficios potenciales de la innovación y las amenazas que el cambio inevitablemente conlleva. Como tal, el apetito de riesgo es único para cada organización (…).
>
> La incorporación del riesgo no financiero a los debates sobre el apetito de riesgo empieza por comprender lo que puede abarcar. De hecho, el gran número de riesgos que se incluyen en esta categoría aumenta las posibilidades de que algunos se pasen por alto o se malinterpreten, lo que subraya la importancia de incorporarlos. (…) (Fundación Latinoamericana de Auditores Internos -FLAI, 2023, p.5).

A partir de este planteamiento se propone una lista (no exhaustiva) de **riesgos no financieros** que las organizaciones pueden considerar de acuerdo con su naturaleza y sector donde se desenvuelve. Se tienen los siguientes: Conformidad, Estratégico, Ciberseguridad, Responsabilidad social, Reputación, Protección de datos, Integridad de los datos, Protección de la propiedad intelectual, Conducta de los empleados, Cultura y ética institucional, Salud pública, Diversidad, igualdad e inclusión, Derechos humanos, Medioambiental (Emisiones de gases de efecto invernadero, Gestión de residuos, Abastecimiento de materias primas, Acceso/gestión de los recursos naturales, Cambio climático).

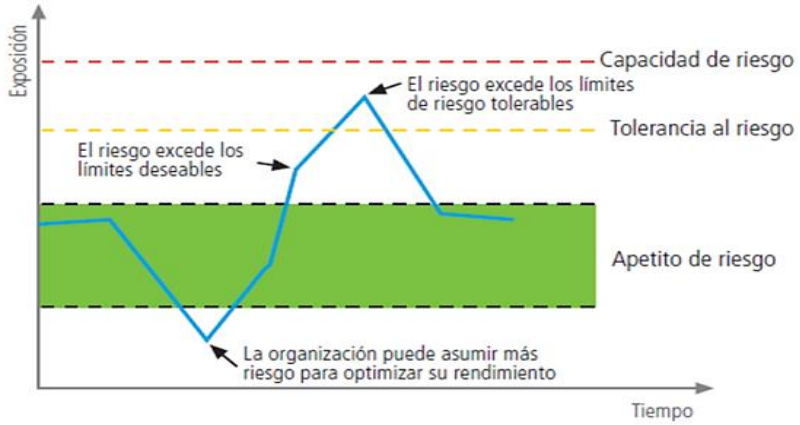
De este modo, será necesario que cada entidad pueda determinar el apetito del riesgo desde una perspectiva cuantitativo o cualitativa, o bien con una combinación de estas que le permita gestionarlo de forma adecuada, siempre atendiendo la normatividad aplicable que rige sus actuaciones para el cumplimiento misional y la protección de los recursos públicos que utiliza para su operación.

Resumiendo, se precisan las siguientes definiciones para efectos de la presente guía:

- **Apetito de riesgo:** es el nivel de riesgo que una entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe gestionar.
- **Tolerancia del riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. (relacionado con la solvencia y liquidez).

Gráficamente, en la figura 12 se puede observar la interrelación entre las anteriores definiciones:

Figura 12 Capacidad, Límites y Tolerancia al Riesgo



Fuente: Superintendencia Financiera de Colombia. 2023

Bajo las anteriores bases conceptuales y este marco que evalúa la Superintendencia Financiera de Colombia a sus entidades y empresas vigiladas, es posible adaptar a cada entidad los elementos de análisis más aplicables, con el fin de establecer el apetito del riesgo y su incorporación a la política para la gestión integral del riesgo, para su aprobación

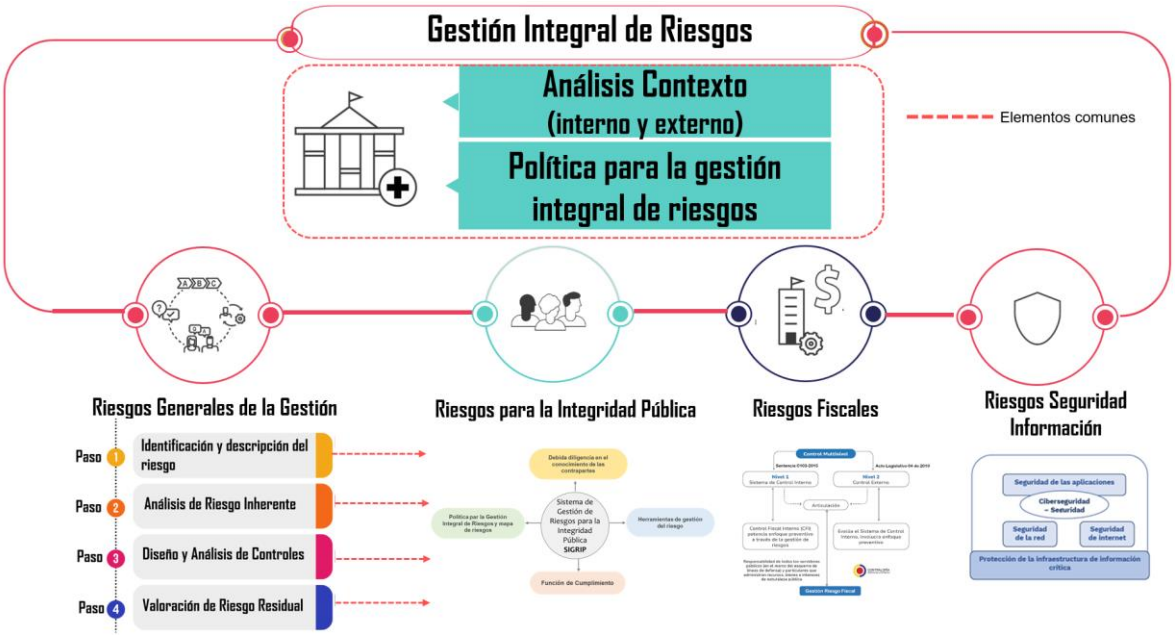
por parte del Comité Institucional de Coordinación de Control Interno, Comité de Auditoría u otra instancia de este mismo nivel jerárquico.

2.5 Articulación ámbitos para la gestión integral de riesgos:

Para el análisis integral de los riesgos que pueden afectar el cumplimiento de las funciones y objetivos de la entidad, donde se involucra, la afectación al patrimonio público, la posible vulneración a activos de información, así como la afectación a la confianza de las múltiples partes interesadas en el uso del entorno digital y aquellas conductas asociadas a comportamientos no éticos que van en contravía del ejercicio íntegro del servicio público, a continuación se muestra gráficamente la articulación de todos estos ámbitos, en el marco general para la gestión integral del riesgo que se despliega en los capítulos siguientes.

La figura 13 muestra los ámbitos que se involucran en la gestión del riesgo, con sus elementos comunes que corresponden al análisis del contexto estratégico interno y externo, la definición de la política para la gestión integral del riesgo y los pasos metodológicos aplicables de i) identificación y descripción del riesgo, ii) análisis del riesgo inherente, iii) diseño y análisis de controles y iv) valoración del riesgo residual, generales para todas las tipologías de riesgo que desarrolla la guía, los cuales se despliegan de forma detallada en el capítulo III.

Figura 13 Articulación ámbitos gestión del riesgo



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

Capítulo III

Riesgos Generales de la Gestión

Teniendo en cuenta la estructura metodológica general, descrita en el punto 2.5 del capítulo anterior, a continuación, se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la operación de la entidad, que en el lenguaje de marcos de referencia internacional podrían llamarse operativos, al ser propios o intrínsecos a las procesos, funciones y misionalidad de cada entidad.

En este sentido, los riesgos que se analicen variarán dependiendo de los diferentes ámbitos organizacionales, bajo la comprensión del modelo de procesos aplicable, de acuerdo con su naturaleza, funciones, estructura organizacional, grupos de valor que atiende, recursos y otras particularidades que permiten cumplir con la misionalidad en cada una de las entidades, en los diferentes órdenes y niveles de la administración pública, lo que implica que la construcción de los mapas de riesgo por proceso podrán variar en número y complejidad, atendiendo el número de procesos, el objetivo y alcance de cada uno y su despliegue en actividades clave, para la entrega de productos y servicios públicos.

Paso 1:* *Identificación y descripción del riesgo

3.1 Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados:

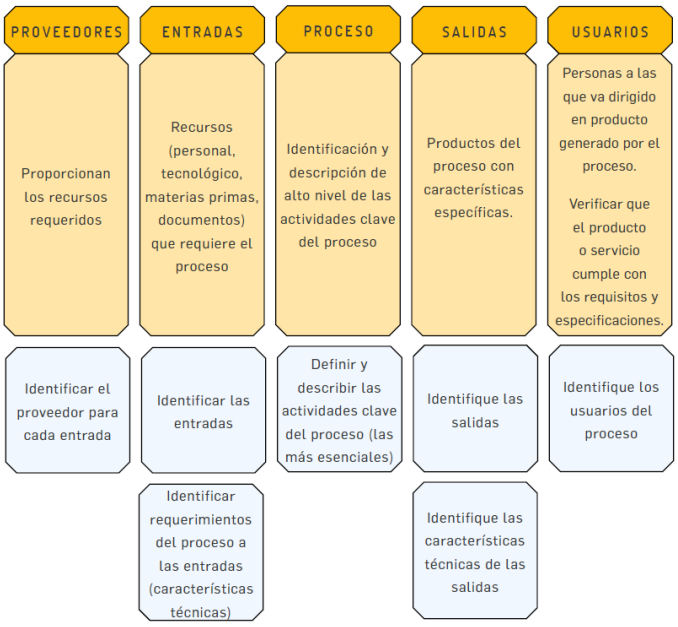
Para una identificación asertiva y precisa de los riesgos claves de cada proceso, deberán considerarse aquellos eventos que podrían afectar de forma previsible el logro de los objetivos de proceso, considerados y ya descritos con los atributos SMART (ver numeral 2.1 Análisis Estratégico de la entidad y su modelo de Operación basada en procesos).

Para llevar a cabo este análisis se debe considerar, adicional al objetivo del proceso, la estructura del mismo con sus actividades clave y la forma como participa dentro de la

cadena de valor o ciclo de los procesos. Al respecto, la Guía para la Gestión por Procesos en el marco de MIPG señala:

> Teniendo en cuenta que las diferentes tareas que se encuentran al interior del ciclo de procesos están interrelacionadas, el orden en el que estas se llevan a cabo puede variar de acuerdo con cómo se conciba cada uno de los procesos. (…) La importancia real de llevar a cabo el ciclo de procesos reside en comprender la interacción de sus diferentes elementos y de las necesidades operativas que cada uno de ellos debe tener. (Función Pública, Guía para la gestión por procesos en el marco de MIPG, 2020, p.55, 56). Cada uno de los componentes del ciclo de procesos se resume a continuación gráficamente (ver figura 14).

Figura 14 Componentes dentro del ciclo de procesos



Fuente: *Función Pública, Dirección de Gestión y Desempeño Institucional, 2019.*

Lo anterior implica que consideren los atributos de los bienes o servicios que podrían verse afectados por diferentes eventos, en el marco de la cadena de valor, "*la cual consiste en*

una serie de insumos, actividades de transformación o procesos para la generación de una serie de productos y servicios o resultados orientados a la satisfacción de una serie de necesidades y requerimientos de sus grupos de valor que fueron definidos previamente y que en sí mismos constituyen una cadena de entrega a través de la cual se produce la transformación necesaria para la producción de productos o servicios". (Función Pública, Guía para la gestión por procesos en el marco de MIPG, 2020, p.60). Esta cadena de valor público se observa en la figura 15.

Figura 15 Cadena de valor público

Fuente: *Función Pública, Dirección de Gestión y Desempeño Institucional, 2017.*

De este modo, para establecer los puntos de riesgo clave en los procesos, es necesario considerar los atributos de los productos, servicios o resultados de procesos que podrían verse afectados dentro del ciclo del proceso que se esté analizando, así como el efecto de estos posibles eventos en el resultado de otros procesos, dentro de una misma cadena de valor.

3.2 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.

3.3 Identificación de áreas de factores de riesgo:

Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

En la Tabla 2 se establece un listado con los factores de riesgo que pueden incidir en un proceso, los cuales podrán ampliarse o adecuarse de acuerdo con las características propias de cada proceso o entidad, sector donde se desenvuelve y otros aspectos que puedan determinar factores adicionales que deban ser contemplados para una adecuada identificación del riesgo. Esta tabla incluye los factores que se describen en el Capítulo VI que desarrolla los riesgos para la integridad pública.

Tabla 2 Factores de riesgo

Factor	Definición		Descriptores
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

Factor	Definición		Descriptores
			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

Factor	Definición		Descriptores
			Hurto 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
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

Factor	Definición		Descriptores
			Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

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

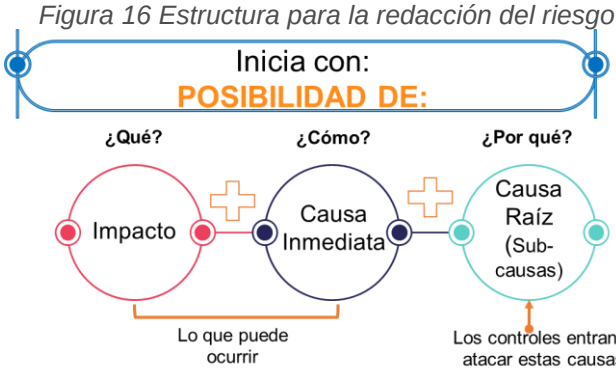
NOTA: *Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con su complejidad, con el sector en el que se desenvuelve, su entorno y otras particularidades organizacionales.*

3.4 Descripción del riesgo:

A partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados, se debe proceder con la descripción del riesgo.

Con el fin de facilitar la redacción adecuada del riesgo y desplegar de todos los detalles necesarios para la identificación, se propone una estructura que se muestra en la figura 16:

Figura 16 Estructura para la redacción del riesgo



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

Desglosando la estructura propuesta tenemos:

 Impacto: las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo.

 Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Estos dos elementos permiten plantear el evento no deseado (¿qué puede ocurrir?), es decir la situación, acción, condición o suceso incierto que, si ocurre, podría afectar el logro de los objetivos de la entidad.

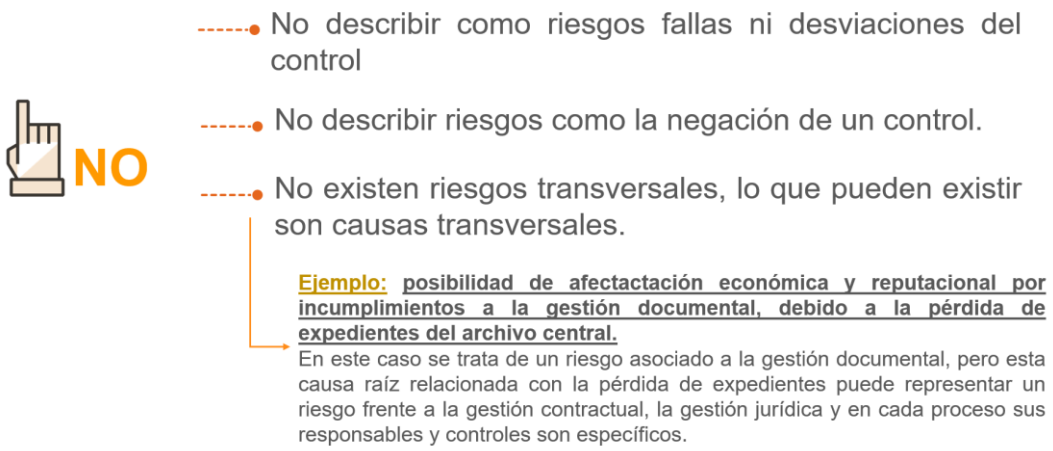
Características clave: Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.

 Causa raíz: Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles en el paso 3 de diseño y análisis de controles. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Las características clave: Identificar causas raíz y condiciones contribuyentes que pueden clasificarse en: humanas, tecnológicas, normativas, ambientales, organizacionales. Un adecuado análisis de causa raíz debe permitir diferenciar la causa raíz, de la causa inmediata, entendida esta última como las circunstancias más evidentes sobre las cuales se presenta el riesgo y que en ocasiones, no constituyen la causa principal del riesgo.

Se recomienda para una adecuada redacción del riesgo, tener en cuenta algunas premisas como las que se muestran en la figura 17 (ver siguiente página).

Figura 17 Premisas para una adecuada redacción del riesgo



Fuente: *Elaboración Dirección de Gestión y Desempeño Institucional. 2025*

Bajo las anteriores consideraciones, 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***

3.5 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.**

Con la aplicación de este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo la actividad que genera la exposición al riesgo identificado y descrito, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Como referente, a continuación, se muestra en la tabla 3 algunas actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Tabla 3 Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Muy Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería ***Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

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

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la **exposición al riesgo** estará asociada al proceso o actividad que se esté analizando, es decir, al **número de veces que se pasa por el punto de riesgo en el periodo de 1 año,** en la tabla 4 se establecen los criterios para definir el nivel de probabilidad.

Tabla 4 Criterios para definir el nivel de probabilidad

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

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

***Nota:** Dependiendo del tamaño y complejidad de los procesos de la entidad, los rangos de análisis de la frecuencia de la actividad de la tabla 4 podrás ser ajustados o adaptados a las necesidades de cada entidad, ampliando las frecuencias, pero siempre manteniendo los niveles y porcentajes asignados, con el fin de no afectar la estructura metodológica.*

3.6 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. Cabe señalar que en versiones anteriores de la guía se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se hace necesario agruparlos en impacto económico y reputacional, con el fin de facilitar el análisis y evitar la subjetividad en los análisis por parte de los líderes internos.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se deberá tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel mayor e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel mayor. En la tabla 5 se establecen los criterios para definir el nivel de impacto.

Tabla 5 Criterios para definir el nivel de impacto

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

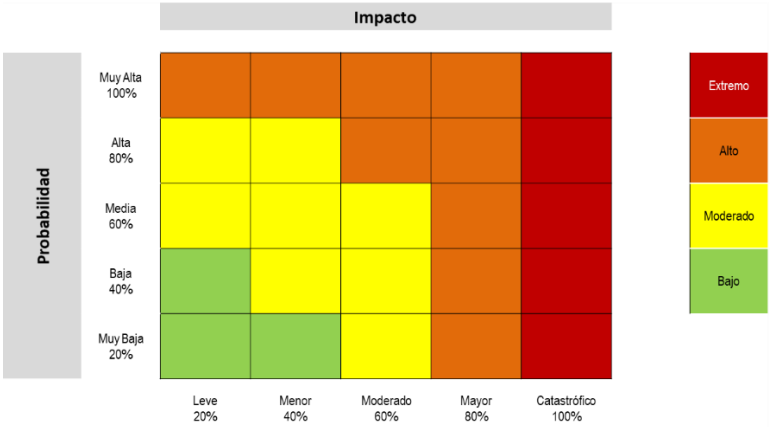
Fuente: Actualizada Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

Nota: *Dependiendo del tamaño y complejidad de los procesos de la entidad, los rangos del análisis de la afectación económica y reputacional de la tabla 5 podrán ser ajustados o adaptados a las necesidades de cada entidad, ampliando los valores en afectación económica; en cuanto a afectación reputacional es viable mantener la estructura propuesta, o bien precisar los aspectos que se consideren pertinentes, pero siempre manteniendo los niveles y porcentajes asignados, con el fin de no afectar la estructura metodológica*

3.7 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 (ver figura 18).

Figura 18 Matriz de calor (niveles de severidad del riesgo)



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

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

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:

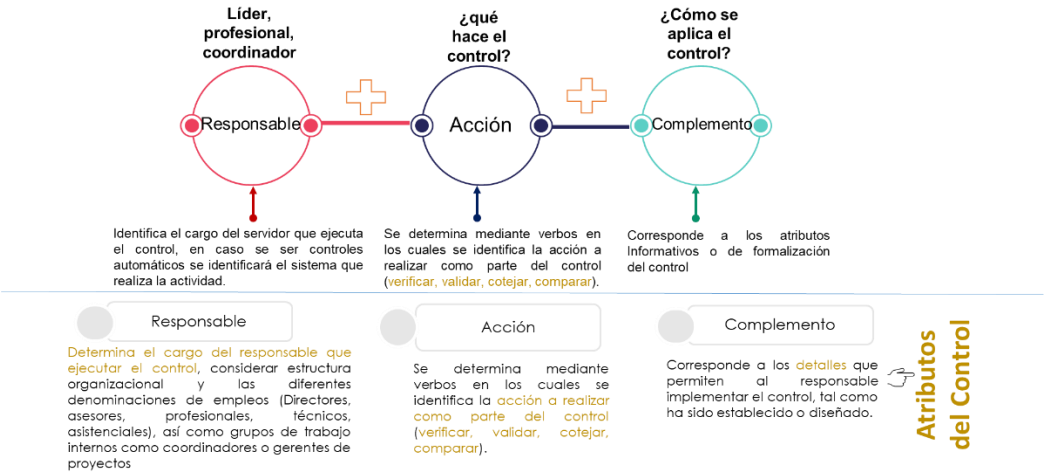
- Estas se pueden diseñar y establecer para cada riesgo a través de diferentes mecanismos, bien sea a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya 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.

- Las actividades de control deberán atender las causas raíz identificadas y enfocarse en la gestión de los factores de riesgo previamente identificados. Estas serán mayormente efectivas cuando cuenten con todos sus atributos y cuando estén directamente relacionadas con tales causas y factores de riesgo.

3.8 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. La estructura propuesta se despliega en la figura 19 que se muestra a continuación:

Figura 19 Estructura para la redacción de controles



Fuente: *Elaboración Dirección de Gestión y Desempeño Institucional. 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.

 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.

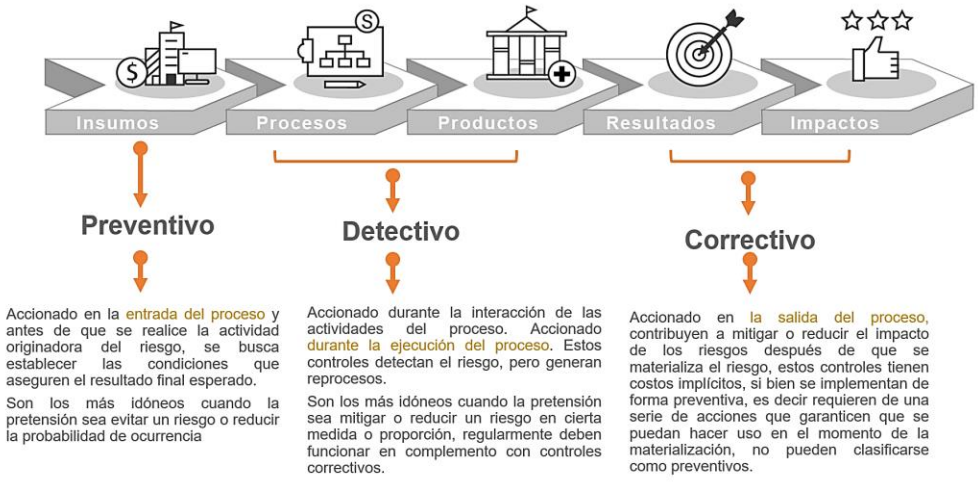
Se tiene entonces que, para la redacción del control es necesario aplicar todos los atributos acá descritos, de manera tal que se constituyan en una herramienta de control efectiva, los cuales se agrupan a través de la estructura para la redacción del control.

3.9 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 más adelante (ver figura 20):

Figura 20 Cadena de valor del proceso y las tipologías de controles



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

De acuerdo con el anterior esquema en el ciclo de un proceso, tenemos las siguientes tipologías de controles:

- **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.
- **Control detectivo:** accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **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.

3.10 Valoración de Controles:

La tabla aplicable para la valoración de controles que se muestra en la tabla 6, determina la forma como se califican los atributos o características de **Eficiencia**, todos los demás atributos informativos o de formalización del control, explicados en el numeral 3.8 Estructura para la Descripción del Control no se aplica valoración, pero deben analizarse para garantizar su el diseño, aspectos listados en la tabla 7.

Tabla 6 Valoración de controles

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

Tabla 7 Análisis atributos formalización del control

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.
	Combinación estructuras documentales y sistemas de información	Se aplican análisis documentales y registros en sistemas de información de apoyo.
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	
	Combinado (manual y electrónico)	

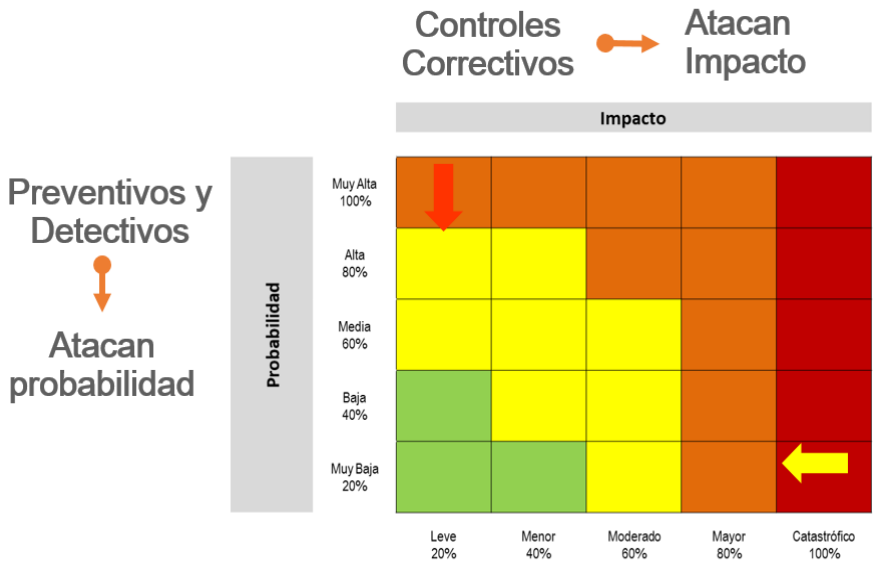
Características de Eficiencia		Descripción
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

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

3.11 Aplicación de Controles en la matriz de severidad:

Teniendo en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor, explicada en el numeral *3.7 Análisis de severidad*, a continuación, en la figura 21 se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Figura 21 Movimiento en la matriz de calor acorde con el tipo de control



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

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.

Para mayor claridad, a continuación, en la tabla 8 se despliega un ejemplo, donde se observan los cálculos requeridos para la aplicación de 2 controles, uno preventivo y uno detectivo, para el caso no se cuenta con controles correctivos.

Tabla 8 Aplicación de controles para establecer el riesgo residual

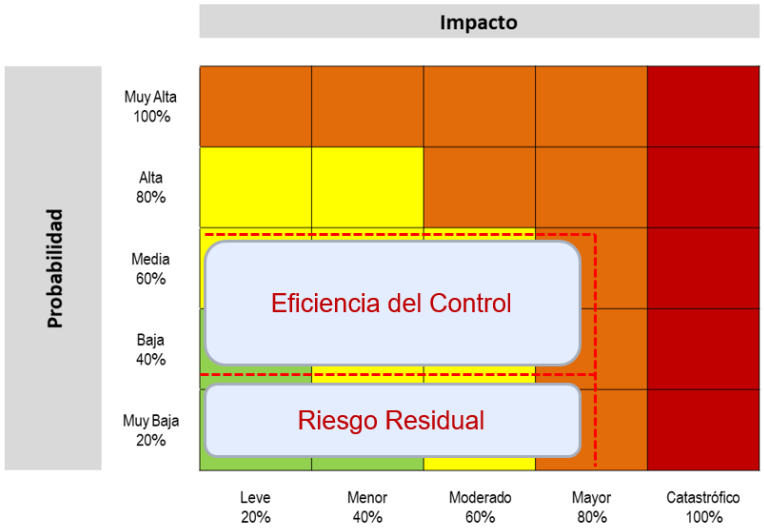
Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2º control				36%
	Valoración control 2 detectivo			30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual				**25,2%**
	Valoración de Impacto				
	Impacto Inherente	80%			

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				80%

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

Gráficamente el movimiento en la matriz de calor se muestra en la figura 22 a continuación:

Figura 22 Movimiento en la matriz de calor con el ejemplo propuesto



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

Una vez aplicada la totalidad de la metodología explicada se procede con la elaboración de los mapas de riesgo por proceso, cuya estructura puede corresponder a una matriz en formato Excel como la que se muestra a continuación en la tabla 9, o bien para aquellas entidades con mayor nivel de complejidad y capacidad institucional puede tener un

desarrollo a través de software especializados, los cuales en todo caso deben mantener la misma línea del esquema metodológico propuesto.

3.12 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.

Nota: *Como parte de la caja de herramientas se despliega un ejemplo bajo un proceso tipo, como referente para la aplicación de la metodología ya explicada, en cada uno de los 4 pasos que permiten la identificación, análisis, valoración y tratamiento de los riesgos.*

Capítulo IV

Gestión Preventiva de Riesgos Fiscales

Este capítulo tiene como finalidad 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 en la tabla 9:

Tabla 9 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) • recaudación • manejo • inversión (de sus rentas)	En orden a cumplir los fines esenciales del Estado, con sujeción a los principios establecidos en artículo 3 de la Ley 610 de 2000

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

Para tener claro el ámbito normativo y jurídico del control fiscal, es necesario precisar que sus bases están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, los cuales fueron modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

La Ley 610 de 2000 establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías y a través del Decreto 403 de 2020 se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.

A partir de lo anterior, el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante el cual tiene carácter excepcional, no vinculante, no implica coadministración, no versa sobre la conveniencia de las decisiones de los administradores de recursos públicos, se realiza en forma de advertencia al gestor fiscal y deberá estar incluido en un sistema general de advertencia público; se busca con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave que se desarrollan a continuación.

4.1 Control fiscal interno y prevención del riesgo fiscal:

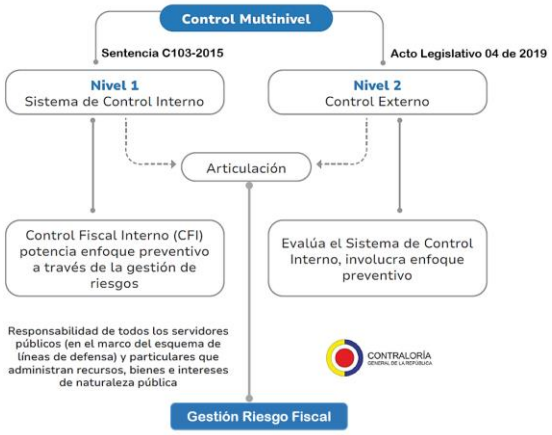
En el nuevo modelo constitucional, el control fiscal adquiere un enfoque preventivo que se potencia con el control interno, a partir de la premisa que el Sistema de Control Interno es el conjunto de mecanismos y medidas que toma una administración para proveer una seguridad razonable respecto al logro de los resultados, con lo cual se brinda también seguridad razonable al gestor fiscal, de haber tomado todas las medidas posibles para evitar daños al patrimonio del Estado.

La denominación de **gestor fiscal** comprende los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros roles cuyas funciones u obligaciones incidan en la gestión fiscal.

Se define entonces un modelo de **control fiscal multinivel**, entendido como la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

El Control Fiscal Interno (CFI) se entiende como el primer nivel para la vigilancia fiscal de los recursos públicos, la prevención de riesgos fiscales y la defensa del patrimonio público. El Control Fiscal Interno hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de aseguramiento, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta. La figura 23 muestra este despliegue y sus elementos de articulación que sustentan el desarrollo del presente capítulo.

Figura 23 Articulación modelo constitucional control fiscal y sistema de control interno



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

A continuación, se presenta el paso a paso de la gestión del riesgo fiscal (identificación, análisis del riesgo inherente, control y valoración del riesgo residual), que debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso.

La metodología que se propone es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses patrimoniales de naturaleza pública, con el fin de prevenir efectos dañosos, lo cual a la vez permite mitigar la posibilidad de afectación al patrimonio por parte de los diferentes gestores fiscales.

Como parte integral de la metodología propuesta, se pone a disposición un Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas (ver anexo), el cual ha sido construido como resultado del análisis de precedentes (aproximadamente 130 fallos con responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República) y debe ser utilizado como marco de referencia para la identificación y valoración de riesgos fiscales, de conformidad con las particularidades de cada entidad (naturaleza, complejidad, recursos, usuarios o grupos de valor, portafolio de productos y servicios, sector en el cual se desenvuelva, entre otros).

De manera complementaria, cada entidad deberá analizar si existen puntos de riesgos y circunstancias inmediatas diferentes a los identificados en dicho catálogo.

4.2 Definición y elementos del riesgo fiscal:

El riesgo fiscal se define de la siguiente manera:

> Efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un ***evento potencial.***

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

Efecto dañoso: es el daño que se generaría sobre los recursos, 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, los bienes y/o los intereses patrimoniales de naturaleza pública.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso (Potencial Daño)

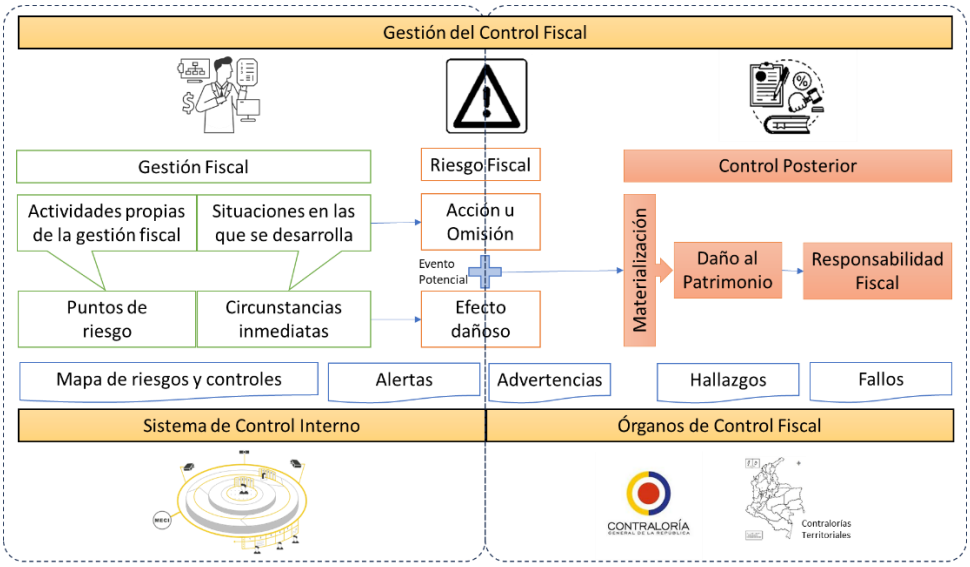
No se debe confundir el riesgo fiscal con el daño patrimonial[4]. El riesgo fiscal se relaciona con el evento de potencial efecto perjudicial sobre los recursos, bienes o intereses públicos, mientras que el daño patrimonial es la afectación real y concreta a los mismos, como resultado de una acción u omisión.

En el modelo multinivel, la gestión del riesgo fiscal corresponde a todos los responsables de la implementación y sostenibilidad del sistema de control interno, mientras que la determinación de hallazgos fiscales y el establecimiento de la responsabilidad sobre el daño patrimonial corresponderá al órgano de control fiscal. Su articulación y especificidad de cada esquema se observa en la figura 24 (siguiente página).

[4] Ley 610 de 2000, artículo 6. Daño patrimonial al Estado: "*lesión del patrimonio público, representada en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado, producida por una gestión fiscal antieconómica, ineficaz, ineficiente e inoportuna, que en términos generales, no se aplique al cumplimiento de los cometidos y de los fines esenciales del Estado, particularizados por el objetivo funcional y organizacional, programa o proyecto de los sujetos de vigilancia y control de las contralorías*.

Dicho daño podrá ocasionarse por acción u omisión de los servidores públicos o por la persona natural o jurídica de derecho privado, que en forma dolosa o culposa produzcan directamente o contribuyan al detrimento al patrimonio público"

Figura 24 Gestión del Control Fiscal



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

4.3 Metodología para el levantamiento del mapa de riesgos fiscales:

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, fundamental para la protección de los recursos, bienes e intereses patrimoniales públicos a cargo de los gestores fiscales (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros), lo cual contribuye al cumplimiento de sus funciones y al aseguramiento razonable para la toma de decisiones.

Si bien este aparte de los riegos fiscales se presenta de forma separada, su incorporación y gestión debe tener un enfoque integral, junto con las demás herramientas e instrumentos diseñados para la gestión del riesgo estratégico y operativo. Por lo que, en aplicación de los 4 pasos metodológicos explicados en el Capítulo III, a continuación, se desarrollan con la especificidad correspondiente.

Paso 1: identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario tener en cuenta los siguientes pasos (ver figura 25).

Figura 25 Pasos para la identificación del riesgo fiscal

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

1.1 <u>Puntos de riesgo y las circunstancias inmediatas</u>

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 (Ley 610 de 2000. 15 de agosto de 2000. Diario Oficial No. 44133), 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 este ejercicio, se sugieren las siguientes preguntas orientadoras, descritas en la tabla 10.

Tabla 10. Preguntas orientadoras para identificar puntos de riesgo fiscal y circunstancias 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. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual 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.	Puntos de riesgo fiscal y circunstancias inmediatas

Preguntas y criterios para la identificación	Sirve para identificar
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, 2025.

1.2 Identificación de 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.

1.1. 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:

(i) Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.

(ii) 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

(iii) Multas impuestas por hechos que no comportan gestión fiscal

(iv) Existencia de actuación de cobro coactivo por parte de la entidad.

(v) 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.

(vi) 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)[5].

1.5 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:

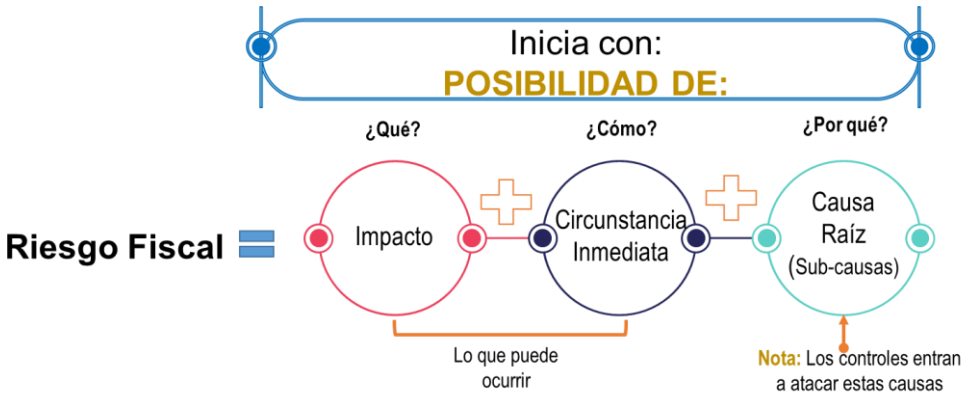
- ✓ Iniciar con la expresión: ***Posibilidad de***, dado que nos estamos refiriendo al evento potencial.

[5] Concepto CGR-OJ-115-2021 de la Contraloría General de la República, pág. 13

- ✓ **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).
- ✓ **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.
- ✓ **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[6].

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales se desarrolla en la figura 26:

Figura 26 Descripción riesgo fiscal



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

Ejemplo 1:

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a

[6] El control fiscal y la responsabilidad fiscal en Colombia. Luz Jimena Duque Botero y Fredy Céspedes Villa. Ibáñez 2018

gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago. A continuación, en la tabla 12 se desarrollan los pasos antes explicados:

Tabla 11 Aplicación pasos descripción riesgo fiscal Ejemplo 1

Paso	Identificación
Punto de Riesgo: (actividad de la gestión fiscal)	Administración de inmuebles en arrendamiento al servicio de la entidad
Circunstancia inmediata: (situación en la que se presenta el riesgo)	Pago de intereses moratorios en contrato de arrendamiento
Área de Impacto: (patrimonio público afectado)	Recursos públicos de la entidad
Efecto económico: (potencial daño al patrimonio)	Disminución de recursos disponibles equivalente al monto pagado por concepto de intereses moratorios
Causa raíz: (potencial acción u omisión)	Omisión de pago oportuno del canon de arrendamiento

Descripción del riesgo:

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los **recursos de la entidad**	por la generación de intereses moratorios en contrato de arrendamiento	a causa de la omisión en el pago oportuno del canon pactado.

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

Conclusión: El hecho generador del daño no es el pago de la deuda ya que esta es una acción diligente que da cumplimiento a una obligación adquirida. La causa raíz corresponde a la omisión de pago oportuno y el riesgo fiscal al potencial daño representado en los intereses moratorios pagados. Ante dicha situación, se requiere la activación de controles correctivos para evitar que se materialice el daño patrimonial (Hallazgo fiscal), tales como

el reembolso del monto correspondiente a los intereses moratorios y controles preventivos para que no se vuelva a presentar la omisión (causa raíz).

Ejemplo 2: Proceso: Recaudo de impuestos

Objetivo: Gestionar los ingresos tributarios establecidos a favor de la entidad, conforme al estatuto tributario y de procedimiento vigente.

Alcance: Inicia con la identificación de hechos gravables, sujetos pasivos y bases de liquidación de los impuestos establecidos a favor de la entidad y culmina con la expedición de paz y salvo a favor del contribuyente.

Tabla 12 Aplicación pasos descripción riesgo fiscal Ejemplo 2

Paso	Identificación
Punto de Riesgo: (actividad de la gestión fiscal)	Gestión de cobro a contribuyentes en mora del pago de sus obligaciones tributarias.
Circunstancia inmediata: (situación en la que se presenta el riesgo)	Prescripción de los términos para la exigibilidad de las obligaciones tributarias.
Área de Impacto: (patrimonio público afectado)	Intereses patrimoniales de la entidad
Efecto económico: (potencial daño al patrimonio)	Menor recaudo de ingresos tributarios establecidos a favor de la entidad
Causa raíz: (potencial acción u omisión)	Errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Descripción del riesgo:

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los **intereses patrimoniales**	por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora	a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

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

Conclusión: El riesgo fiscal existe desde el momento en que, existiendo obligaciones en mora, los procedimientos de cobro no se ejecutan de manera oportuna y correcta, pues allí surge la potencial reducción del recaudo. En esta etapa, el sistema de control interno debe ser capaz de tomar los correctivos necesarios, pues una vez se materialice la prescripción, se configura el daño patrimonial (hallazgo fiscal) a partir del cual el órgano de control fiscal procede a establecer y exigir la responsabilidad del gestor fiscal.

A continuación, en la tabla 13 se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso.

Tabla 13 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la implementación y operación de redes eléctricas seguras.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por negación del reconocimiento de siniestros en el contrato de seguro, a causa de la omisión en la actualización del inventario de bienes amparados.

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por pérdida, extravío o hurto de bienes muebles de la entidad a causa de la inexistencia de procedimientos documentados para el ingreso y salida de bienes del almacén	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por por menores ingresos percibidos sobre la explotación de marcas de propiedad comercial de la entidad a causa de errores u omisiones en el análisis técnico, jurídico y económico del mercado

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 definidas en los numerales 3.5, 3.6 y 3.7 de la presente guía, 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. Se aplican los lineamientos para la redacción del control establecidos en los numerales 3.8 y 3.9 y tabla definida en el numeral 3.10 de la presente guía.

Ejemplo 3:

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que en cada entidad la cantidad y valor de los bienes muebles en el inventario puede ser muy diversa, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más detallado que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.

Aplicando las tablas de probabilidad e impacto tenemos:

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

→ La actividad se realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es **Media**.

Para determinar el impacto es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

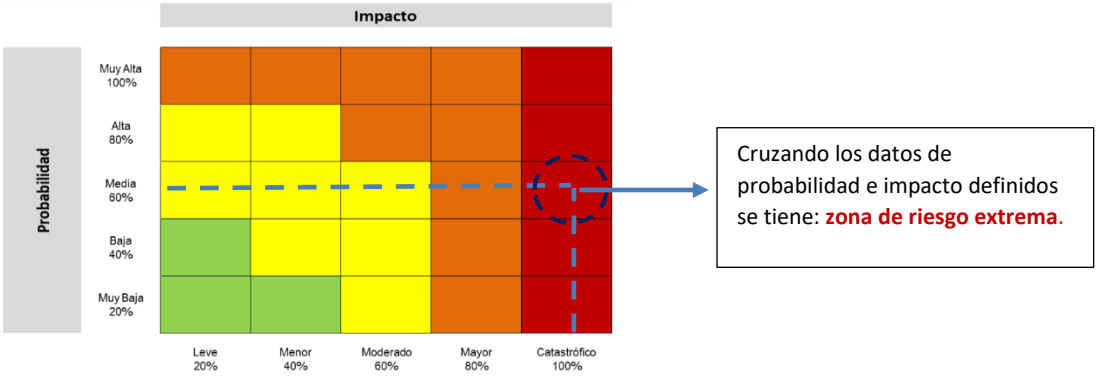
En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que se determina en 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico.

Nivel de Impacto	Afectación Económica
Leve-20%	Afectación menor a 10 SMLMV
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV
Mayor-80%	Mayor a 100 SMLMV y Menor a 500 SMLMV
Catastrófico-100%	Mayor a 500 SMLMV

→ La afectación económica se calcula en más de 500 SMLMV, el impacto del riesgo es **Catastrófico**

Probabilidad inherente= moderada 60%, **Impacto inherente:** catastrófico 100%

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo extremo.



Controles Identificados:

- ✓ Control 1 Preventivo: El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.
- ✓ Control 2 Detectivo: El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.
- ✓ Control 3 Correctivo: El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador

Aplicando la tabla de valoración de controles tenemos:

Control 1	Criterios de efectividad			Peso
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 1 =40%			
Control 2	**Criterios de efectividad**			**Peso**
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y	Tipo	Preventivo		
		Detectivo	x	15%
		Correctivo		

ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 2 = 30%			
Control 3	**Criterios de efectividad**			**Peso**
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	x	10%
	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 3 = 25%			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde 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 y su respectiva valoración, a fin de determinar el riesgo residual.

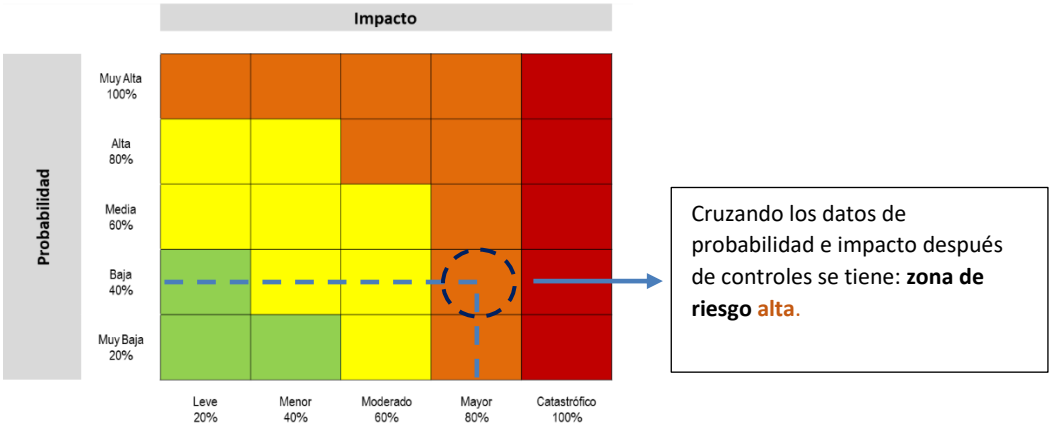
Nivel de riesgo (riesgo residual): Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles, se debe tener en cuenta que, estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Para mayor claridad a continuación, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de efectos dañoso sobre bienes públicos *(área de impacto)*, **por** pérdida, extravío o hurto de bienes muebles de la entidad *(circunstancia inmediata)*, **a causa de** la omisión de cumplimiento del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% =24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	**36%**	Valoración control 2 Detectivo	30%	36%* 30% =10.8% 36% - 10,8% **= 25,2%**
	Probabilidad Residual: 25,2%				

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
información a quien gestiona las pólizas cuando haya lugar *(causa raíz)*.	Impacto Inherente	100%	Valoración control correctivo	25%	100%* 25% =25% 100% - 25% = 75%
	Impacto Residual: 75%				

Teniendo 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 y cálculo final:



La anterior información puede trasladarse a la matriz mapa de riesgo que hace parte de los anexos desarrollados para la presente guía.

Capítulo V

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.

Este capítulo aborda temas como la identificación de activos de información, riesgos, amenazas y vulnerabilidades, para llevar a cabo un análisis de los riesgos de seguridad de la información, luego, la implementación de controles diseñados para mitigar estos riesgos y el proceso de reporte de estos.

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.

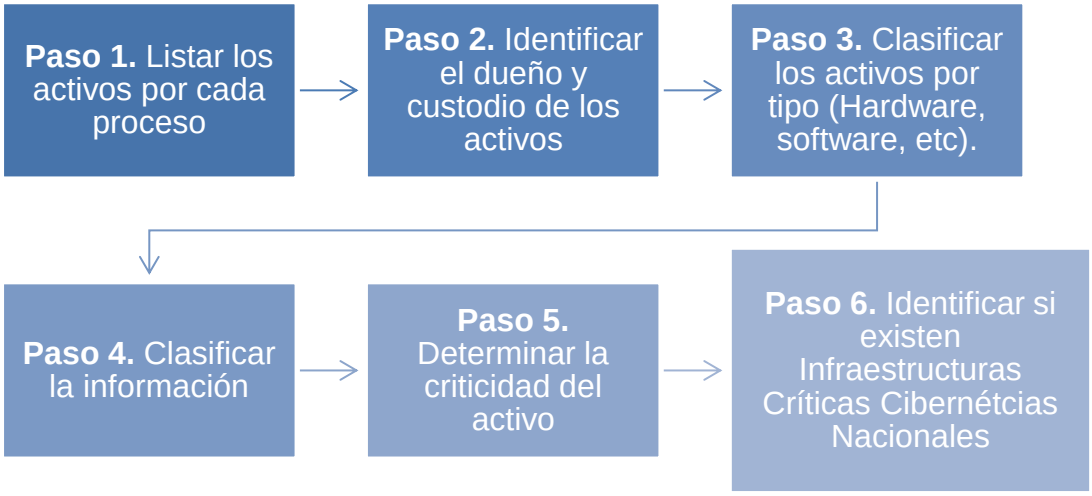
***Paso 1:* Identificación y descripción de riesgos de seguridad de la información**

5.1 Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados:

En primer lugar, se deben identificar los activos de Información[7] mediante las actividades descritas en los "*Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica 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 listados en la figura 27:

Figura 27 Pasos para la identificación y valoración de activos



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

[7] Identificación del activo de información (Ley 594 de 2000 - Ley 1712 de 2014- Decreto 103 de 2015 - Decreto 1080 de 2015 - ISO 27001)

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:

    - **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
    - **Sistemas de información y aplicaciones de Software**: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
    - **Dispositivos de Tecnologías de información- Hardware**: Equipos de cómputo que por su criticidad son considerados activos de información, no sólo activos fijos.
    - **Soporte para almacenamiento de información**: Equipo para almacenamiento de información como USB, Discos Duros, CDs, SAN, NAS.
    - **Servicios**: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
    - **Recursos Humanos**
    - **Instalaciones**
    - **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:
  - **Físico** (análogo)
  - **Digital** (electrónico) Este campo se diligencia si el Tipo de activo es "Información"
  - **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.

Tabla 14 Criterios de Clasificación

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 en la tabla 14:

Tabla 15 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 Critica cibernética Nacional**: Se define si el activo corresponde con los criterios de Infraestructura Critica 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.
  - **Publicada**: Si la información es publica y se puede consultar en un sitio web (interno o externo) o un sistema de información del Estado.
  - **Publicada** (Interno - Intranet)
  - **Publicada** (Externo - Internet)
  - **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.

Tabla 16 Clasificación de Activos

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)						
Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	Es Infraestructura Critica 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, cobija 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, articulo, 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 cobija 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.

Tabla 17 Índice de Información Clasificada y Reservada

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:

    - **Dato personal público**: Toda información personal que es de conocimiento libre y abierto para el público en general. Ejemplo: Número de identificación apellidos.
    - **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 Nº teléfono.
    - **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.

Tabla 18 Datos Personales

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.

"*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.

A continuación, se desarrolla un ejemplo práctico:

i) Listado y registro de activos, asociando macroproceso, proceso, identificador, tipo, serie y subserie documental:

Macroproceso	Proceso	Identificador	Tipo	Oficina	Serie documental	Subserie documental
Gestión Financiera	Gestión de nomina	GF001	Software	Financiera	001	00001
Gestión Financiera	Gestión de nomina	GF001	Software	Financiera	001	00001

ii) Datos sobre el activo de información, sus responsables, soportes de almacenamiento de información, servicios, soporte registro, medio conservación, idioma.

Nombre	Descripción	Nombre del responsable de la producción de la información (Propietario del activo)	Fecha de generación de la información	Nombre del responsable de la información (Custodio del activo)
Software de gestión de nómina (Pagosnet)	Software de gestión de nomina	Director TI	12/03/2025	Analista nomina
Informe pagos de nómina periodo: ene-2025 a marzo-2025	Informe de los pagos de nómina realizados den el periodo: ene-2025 a marzo-2025	Director Financiero	12/03/2025	Analista nomina
Fecha de ingreso del activo al archivo	**Soporte de registro**	**Medio de conservación**	**Formato**	**Idioma**
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español

iii) Clasificación de los activos, de acuerdo con el análisis sobre el nivel de criticidad para cada uno:

Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	¿Es Infraestructura Critica Cibernética?	Información publicada	Lugar de consulta o ubicación
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Intranet
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Sharepoint

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
N/A	N/A	N/A	N/A	N/A	N/A
Si	artículo 18 de la ley 1712 de 2014	artículo 18 de la ley 1712 de 2014	Reserva parcial	15/03/2025	15 años

¿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
N/A	N/A	N/A	N/A	N/A
Si	No	Dato semiprivado	Realizar el pago de nomina	Si

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

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:

Tabla 19 Matriz de Riesgos de Seguridad de la Información

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:

- ✓ Información
- ✓ Software
- ✓ Hardware
- ✓ Servicios
- ✓ Intangibles
- ✓ Infraestructura crítica cibernética nacional
- ✓ Recursos humanos
- ✓ Instalaciones y Otros Servicios

5.2 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.

5.3 Identificación de áreas de factores de riesgo

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

Tabla 20 Amenazas y Vulnerabilidades

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)

Tabla 21 Tabla de amenazas comunes

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
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida 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
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D

Tipo	Amenaza	Origen
	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).

Tabla 22 Tabla de Vulnerabilidades Comunes

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
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)

Tipo	Vulnerabilidades
	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

5.4 Descripción del riesgo

En este paso se identifican:

Tabla 23 Riesgos de Seguridad de la Información

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.

"*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*."

Si requiere información adicional remitirse al punto 3.4 de esta misma guía.

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 establecidas en el numeral 3.5 del capítulo IV que desarrolla los lineamientos para los riesgos generales de la gestión.

5.5 Determinar la probabilidad

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

Tabla 24 Frecuencia

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

Fuente: Elaboración 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. (Ver tabla 4, capítulo IV, Criterios para definir el nivel de probabilidad)

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. (Ver tabla 4 capítulo III, Criterios para definir el nivel de probabilidad)

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

5.6 Determinar el impacto

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

Tabla 25 Impacto

IMPACTO	
% Impacto Inherente	Impacto Inherente

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

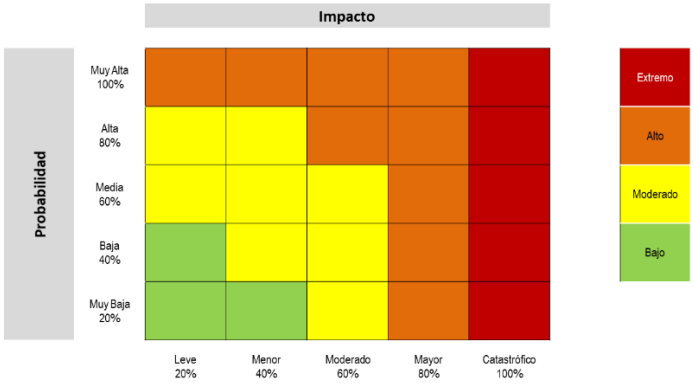
% Impacto Inherente: Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa. (Ver tabla 5 capítulo IV, Criterios para definir el nivel de impacto).

Impacto Inherente: Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa. (Ver tabla 5, capítulo III, Criterios para definir el nivel de impacto).

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

5.7 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. (Figura 17, capítulo IV).



Paso 3: ***Diseño y Análisis de Controles***

5.8 Estructura para la Descripción del Control

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

Tabla 26 Controles

No. Control	Control Anexo A	Descripción del Control

Fuente: Elaboración 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.*

5.9 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.

Tabla 27 Afectación

AFECTACIÓN	
Probabilidad	Impacto

Fuente: Elaboración 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, de acuerdo con la Tabla 7 (Capítulo III) y su valoración mediante la Tabla 6 (Capítulo III).

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	

Características de Eficiencia		Descripción
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.

Tabla 28 Atributos

ATRIBUTOS							
Tipo	**%**	**Implementación**	**%**	**Calificación del control**	**Documentación**	**Frecuencia**	**Evidencia**

Fuente: Elaboración 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, teniendo en cuenta la Tabla 7 Aplicación de controles para establecer el riesgo residual.

Tabla 29 Valoración del Riesgo Residual

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

Fuente: Elaboración 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:

Tabla 30 Plan de Implementación de Controles

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

Fuente: Elaboración 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.*

Capítulo VI

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.

6.1. 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 promocione 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.

6.2. 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 pública[8]. 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:

6.2.1. 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.

[8] OCDE (2020), Manual de la OCDE sobre Integridad Pública, OECD Publishing, Paris, https://doi.org/10.1787/8a2fac21-es.
[9] Definición de soborno según la norma ISO 37001:2025 - Sistemas de gestión antisoborno. Requisitos con orientación para su uso.

6.2.2. Fraude

El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros[10]. 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.

6.2.3. Inadecuada gestión del conflicto de intereses:

Un conflicto de intereses[11] 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.

[10] Concepto construido a partir de los términos y definiciones utilizados por la Organización Internacional de Normalización (ISO, por sus siglas en inglés).
[11] Concepto construido a partir de lo establecido en el artículo 44 de la Ley 1952 de 2019, *"Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario"*

6.2.4. 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"*[12].

6.2.5. 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.

6.3. 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

[12] Según el artículo 2.1.4.3.1.3 del Decreto 1081 de 2015.

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.

6.3.1. 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 (ver numeral 2.3.3). 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.

6.3.2. 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 (ver

numeral 2.3.4). Además, en la sección 1.2 de este documento, 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 en Tabla 31 a continuación:

Tabla 31 Roles y responsabilidades SIGRIP

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	Auditor del Programa	Administrador del Programa	Ejecutores del Programa
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno	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
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 que se desarrolla en el numeral 6.3.7.3	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.

6.3.3. 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 (ver numeral 2.3.1) y un alcance (ver numeral 2.3.2), así como establecer marco de apetito del riesgo (ver numeral

2.4) y el esquema metodológico que aplicarán (ver numeral 2.3.5), 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 el capítulo III, numeral 3.1 y posteriores de esta Guía.

6.3.4. 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. Para estos fines, referirse al numeral 6.3.7.3 de esta Guía.

- ✓ 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:

    - Los objetivos y alcance del Sistema;
    - Cada uno se sus elementos;
    - Los beneficios que tiene el Sistema para la organización
    - 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.

6.3.5. Operación

Como se indició 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 en la figura 28 a continuación.

Figura 28 Sistema de Gestión de Riesgos para la Integridad Pública

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.

6.3.5.1. 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 el Capítulo 3 de la presente Guía. Lo anterior, sin perjuicio de que la metodología pueda ser complementada u objeto de desarrollo por parte de la entidad. Esta Guía 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. **Respecto 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.

Respecto 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. **Respecto 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 en el numeral 3.6 de esta Guía, de forma que pueda aplicarse la Tabla 5, determinada 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[13] es involucrada en procesos que puedan derivar en una sanción y el contagio se da cuando la involucrada es la parte relacionada[14]. 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 prejuzgamiento.

[13] Ver Glosario términos numeral IV. Conceptos clave para la gestión de Riesgos a la Integridad Pública
[14] Ver Glosario términos numeral IV. Conceptos clave para la gestión de Riesgos a la Integridad Pública

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*[15]*"*, 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. Respecto 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.

[15] El uso de este término debe entenderse como el conjunto de actividades y procedimientos que mantienen en niveles aceptables el funcionamiento de la misionalidad de la Entidad y la prestación de sus servicios durante eventos que impidan de manera significativa sus procesos normales.

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 7 de esta Guía, sobre indicadores clave de riesgo.

Respecto de la Tabla 2 de “Factores de Riesgo” definida en el numeral 3.3 de la presente guía, se han incorporado los antes descritos para el análisis de los riesgos LA/FT/FP y de integridad pública, los cuales podrán complementarse con las adaptaciones que realice la entidad.

4. Respecto de la "Descripción del riesgo"

La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en el numeral 3.4 de esta Guía. Todos iniciarán con la formula *"Posibilidad de"*, y deben señalar el impacto, la causa inmediata y la causa raíz.

Teniendo en cuenta las amenazas descritas en el numeral 6.2, 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 en la tabla 32 a continuación:

Tabla 32 Ejemplos como referente para análisis del riesgo

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	

Impacto	Causa inmediata		Causa raíz
		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 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, como se explica en la tabla 33.

Tabla 33 Análisis riesgos LA/FT/FP

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 Capítulo III de la presente guía, específicamente en los numerales 3.5 y 3.6, con las correspondientes Tablas 4 y 5, 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 definida en el numeral 3.7, 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 Capítulo III de esta Guía, específicamente en lo definido en el numeral 3.8 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 Capítulo III de la presente guía.

6.3.5.2. 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.

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 [proporcionalidad].

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 elaboré 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 control[16].
    d. En el caso de personas jurídicas u otras estructuras, identificar los beneficiarios finales[17].
    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.

[16] Según los artículos 260 y 261 del Código de Comercio Colombiano.
[17] Según el artículo 631-5 del Estatuto Tributario Colombiano, son beneficiarios finales *"la(s) persona(s) natural(es) que finalmente posee(n) o controla(n), directa o indirectamente, a un cliente y/o la persona natural en cuyo nombre se realiza una transacción. Incluye también a la(s) persona(s) natural(es) que ejerzan el control efectivo y/o final, directa o indirectamente, sobre una persona jurídica u otra estructura sin personería jurídica".* En el resto del artículo se detallan los demás atributos para tener en cuenta en la identificación del beneficiario final.

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 en esta Guía es enunciativo. En el Manual, cada 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 “posdebida 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.
    a. 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, de que trata el numeral 6.3.5.4 de esta Guía, 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.

6.3.5.3. Función de cumplimiento

La función de cumplimiento implica, entre otros aspectos:

- ✓ 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.
- ✓ 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.
- ✓ 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.

- ✓ Promover la adopción de correctivos del SIGRIP y adoptar aquellos que estén dentro de su competencia.
- ✓ 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.
- ✓ Proponer a la Alta Dirección la actualización de los elementos del SIGRIP y velar por su comunicación oportuna a todas las partes interesadas.
- ✓ Colaborar con el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos que requiera el SIGRIP y aplicarlos según corresponda.
- ✓ Establecer los lineamientos institucionales para la aplicación proporcional basada en riesgos de los mecanismos de debida diligencia en el conocimiento de las contrapartes.
- ✓ Elaborar y someter a aprobación de la Alta Dirección, los criterios objetivos para la determinación de las operaciones inusuales y sospechosas.
- ✓ 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" [18]. 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"* [19].

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:

- ✓ 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.
- ✓ 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.
- ✓ 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.

[18] Artículo 2.2.2.2.1 del Decreto 1083 de 2015.
[19] Artículo 2.2.2.2.2 del Decreto 1083 de 2015.

- ✓ 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.

- ✓ 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.

- ✓ 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 acudirse 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.

6.3.5.4. 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; promocione 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; promocione 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; promocione 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[20].

6.3.6. 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:

- ✓ 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

[20] Se entenderá que cuentan con una Política Antisoborno, Política Antifraude y un Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético, las entidades certificadas en Sistemas de Gestión estructurados de conformidad con los lineamientos dados por la Organización Internacional de Normalización (ISO, por sus siglas en ingles).

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.

- ✓ 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.

- ✓ 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 independencia 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.

- ✓ 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.

Capítulo VII

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.*

Capítulo VIII

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

Teniendo en cuenta lo expresado en el capítulo II 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 7 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.

9.1 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 figura 29.

Figura 29 Definición del tipo de evaluación y los indicadores asociados

Fuente: Departamento Administrativo de la Función Pública, 2018

En este sentido, de acuerdo con la estructura propuesta en la figura 30 se observa la forma como se vinculan los Indicadores Clave de Riesgo articulados con los Indicadores Clave de Proceso.

Figura 30 Articulación Indicadores Clave de Riesgo y 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.

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).

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.

9.2. 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. En la tabla 34 se analizan las características de cada uno.

Tabla 34 Alcance aplicación KPI y KRI

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.

Indicadores Clave de Proceso *(KPI)*	Indicadores Clave de Riesgo (KRI)
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.

9.3 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 en la figura 31:

Figura 31 Pasos para la construcción de Indicadores Clave de Riesgos (KRI)

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 en la Tabla 35:

Tabla 35 Ejemplo Indicadores Clave Riesgo (KRI)

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

Fuente: Adaptado del listado de indicadores y métricas (www.riesgoscero.com) por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

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 delo 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.

Ejemplo

Supongamos que el apetito de riesgo de una entidad ha fijado que el número de quejas de los usuarios puede ser de hasta 10 quejas al mes sin que eso genere una intervención.

Si el KRI revela que se han presentado 8 quejas, significa que la entidad está muy cerca del umbral (10), aumentando el riesgo de que el asunto se pueda salir de control.

Si el KRI llega a 12 quejas, significa que el riesgo ha excedido el apetito y será necesario implementar medidas correctivas.

Finalmente, se debe considerar que, si bien los umbrales de alerta en primera instancia son definidos por los líderes de los procesos, planes, programas y proyectos, dado que son

ellos quienes conocen en mayor detalle su operatividad, estos deberán ser analizados y aprobados por la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno.

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.

9.4 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 (Ver Tabla 36).

Tabla 36 Seguimiento y monitoreo Indicadores Clave de Riesgo (KRI)en el marco del Esquema de Líneas de Aseguramiento

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 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)

Líneas de aseguramiento	Responsable	Responsabilidad frente a 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. • 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

Líneas de aseguramiento	Responsable	Responsabilidad frente a los Indicadores Clave de Riesgo (KRI)
		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

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?lServicio=Tools2&lTipo=descargas&lFuncion=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

COSO (2010). Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks. Research Commissioned by the Committee of Sponsoring Organizations of the Treadway Commission.

Armijo, Mariela. (2011). Planificación estratégica e indicadores de desempeño en el sector público. CEPAL. 2011. https://repositorio.cepal.org/server/api/core/bitstreams/dfa8d5f1-7315-4f10-9824-8fa5b005cc1b/content

Universidad Internacional de La Rioja. (2024). Indicadores clave para la gestión del riesgo en las organizaciones. UNIR Ecuador. https://ecuador.unir.net/actualidad-unir/indicadores-clave-riesgo/

Delfiner, M., & Pailhé, C. (2008). Técnicas cualitativas para la gestión del riesgo operacional. BCRA.

Contraloría General de la República. (2023). Cartilla para el fortalecimiento de hallazgos con incidencia fiscal 2023. Contraloría Delegada para Responsabilidad Fiscal, Intervención Judicial y Cobro Coactivo. https://www.ascontrol.org/sites/default/files/estandar/2023/08/Cartilla%20para%20el%20Fortalecimiento%20de%20Hallazgos%20con%20Incidencia%20Fiscal%202023.pdf

OCDE (2020), Manual de la OCDE sobre Integridad Pública, OECD Publishing, Paris, https://doi.org/10.1787/8a2fac21-es

Organización Internacional de Normalización (ISO). (2025). ISO 37001. Sistemas de gestión antisoborno. Requisitos con orientación para su uso.

Anexos

Anexo 1: Matriz mapa riesgos parametrizada

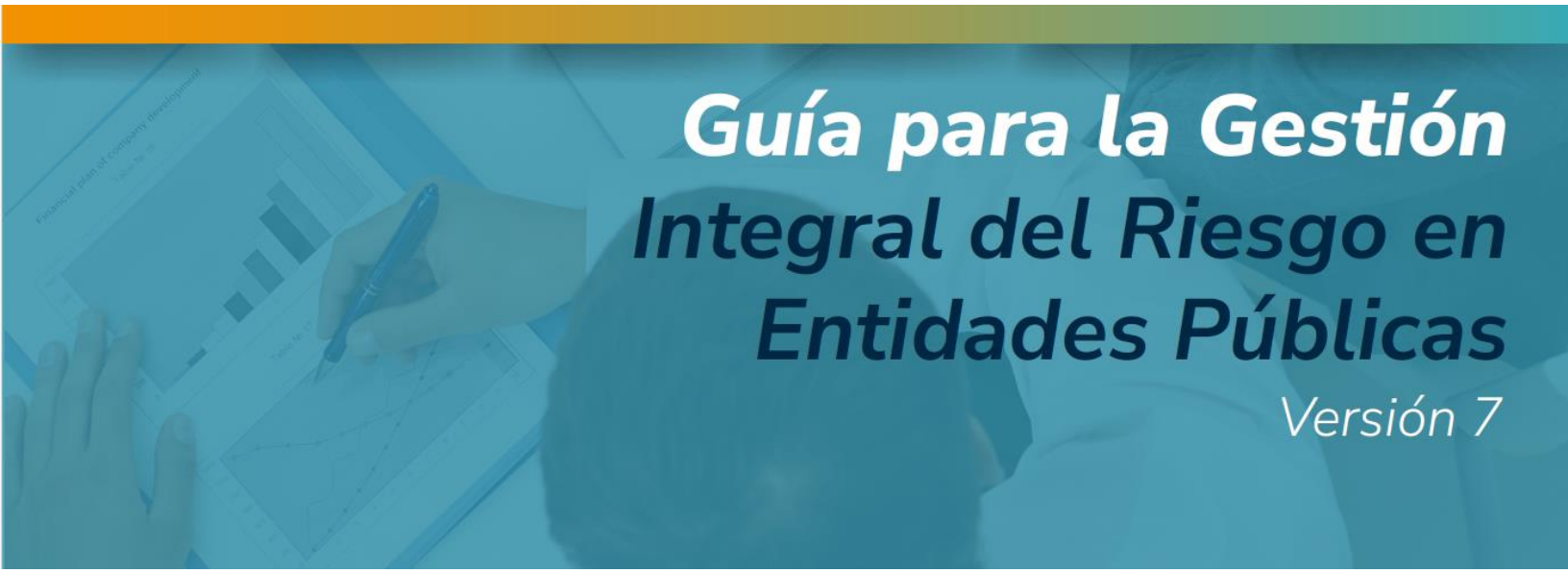
Anexo 2: Glosario

Anexo 3: Catálogo indicativo de puntos de riesgo fiscal

Anexo 4: Matriz estado de madurez de la gestión del riesgo parametrizada

Anexo 5: Matriz Riesgos de Seguridad de la Información

Función Pública



Guía para la Gestión Integral del Riesgo en Entidades Públicas

Versión 7

Carrera 6 No, 12-62
Bogotá D.C. Colombia
Teléfono: **601 7395656**
Fax: **601 7395657**
Página web: **www.funcionpublica.gov.co**
Email**: eva@funcionpublica.gov.co**