ALCALDÍA DE CARTAGO

POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

OFICINA DE GESTION Y DESEMPEÑO INSTITUCIONAL

COPIA CONTROLADA

CUADRO DE CONTROL

ELABORÓ	REVISÓ	APROBÓ
MANUEL HUMBERTO VILLAMIL GONZÁLEZ Técnico Administrativo	VIVIANA RAYO TAMAYO Jefe Oficina Gestión y Desempeño Institucional	VIVIANA RAYO TAMAYO Jefe Oficina Gestión y Desempeño Institucional

CONTROL DE CAMBIOS DE DOCUMENTOS

VERSIÓN	ORIGEN DE LOS CAMBIOS	FECHA DE REGISTRO			NOMBRE DEL FUNCIONARIO
		DIA	MES	AÑO	
1	Creación Política Administración del Riesgo	03	10	2022	Manuel Humberto Villamil González Técnico Administrativo
2	Actualización Política Administración del Riesgo, inclusión Riesgos Fiscales	06	03	2024	Manuel Humberto Villamil González Técnico Administrativo
3	Actualización del documento, pasa de llamarse Política Administración del Riesgo a Política para la Gestión del Integral del Riesgo, acorde a lo establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas en su Versión 7 Se incluye 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	02	01	2026	Manuel Humberto Villamil González Técnico Administrativo

COPIA CONTROLADA

TABLA DE CONTENIDO

1. CONCEPTOS BASICOS: 5
2. NORMATIVIDAD 14
3. OBJETIVO 15
4. ALCANCE 15
5. MARCO DE REFERENCIA 15
6. INSTITUCIONALIDAD 17
7. NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS 18
8. BENEFICIOS APLICACIÓN DE LA POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DEL RIESGO 21
9. METODOLOGIA PARA LA ADMINISTRACION DE RIESGOS 22
10. LINIEAMIENTOS DE LA POLITICA DEL RIESGO 23
11. MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO 24
11.1. Determinación de la Capacidad De Riesgo 24
11.2. Determinación del Apetito de Riesgo 25
11.3 Tolerancia de Riesgo 25
12. IDENTIFICACION DEL RIESGO 26
12.1. Análisis de objetivos estratégicos y de los procesos: 26
12.2. Identificación de los puntos de riesgo: 26
12.3. Identificación Área de impacto: 27
12.4. Identificación de áreas de factores de riesgo: 27
12.5. Descripción del Riesgo 27
13. VALORACION DEL RIESGO 30
13.1. Análisis De Riesgos 31
13.2. Evaluación de Riesgos 35
13.3 Valoración de Controles 36
13.4. Tipología de controles y los procesos: 37
13.5. Análisis y evaluación de los controles: 38
13.6. Nivel de Riesgo (Riesgo Residual): 39
13.7. Estrategias para combatir el riesgo: 39
14. LINEAMIENTOS PARA EL TRATAMIENTO DE RIESGOS FISCALES 40
14.1. Control fiscal interno y prevención del riesgo fiscal 40
14.2. Definición y elementos del riesgo fiscal: 41
14.3. Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales: . 42
15. TRATAMIENTO RIESGOS DE CORRUPCIÓN 45
15.1. Zona de riego y tratamiento 48
15.2. Directrices de redacción para riesgos de corrupción. 48

COPIA CONTROLADA

15.3. Valoración de Riesgos de Corrupción 49
15.3.1. Análisis de la probabilidad 49
15.3.2. Análisis del impacto 50
15.3.3. Análisis del impacto en riesgos de corrupción 51
15.3.4. Tratamiento del riesgo 52
15.3.5. Monitoreo de riesgos de corrupción 53
15.3.6. Reporte de la gestión del riesgo de corrupción 54
15.3.7. Seguimiento de riesgos de corrupción 54
15.3.8. Acciones a seguir en caso de materialización de riesgos de corrupción 54
16. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 55
17. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA - SIGRIP 57
17.1. Integridad Pública 57
17.2. Amenazas Para La Integridad Pública 58
17.2.1. Soborno 58
17.2.2. Fraude 59
17.2.3. Inadecuada Gestión del Conflicto de Intereses 59
17.2.4. Corrupción 59
17.2.5. Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP 60
17.3. SISTEMA DE GESTIÓN DEL RIESGO 60
17.3.1. Contexto de la organización 61
17.3.2. Liderazgo del Sistema 63
17.3.3. Planificación 64
17.3.4. Apoyo 64
17.3.5. Operación 66
17.3.5.1. Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos 67
17.3.5.2. Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos 75
17.3.5.3. Función de Cumplimiento 83
17.3.5.4. Herramientas de gestión del riesgo 87
17.3.6. Monitoreo, evaluación, auditoría y mejora 90

COPIA CONTROLADA

1. CONCEPTOS BASICOS:

RIESGO: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

RIESGO DE CORRUPCIÓN: Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

RIESGO FISCAL: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

GESTIÓN DEL RIESGO FISCAL: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

GESTOR PÚBLICO: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales" A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

GESTOR FISCAL: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus

COPIA CONTROLADA

rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)4" . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

BIEN PÚBLICO: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:
a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.
Ejemplos: Las calles, plazas, puentes, vías, parques etc.
b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.
Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

INTERESES PATRIMONIALES DE NATURALEZA PÚBLICA: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.
Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

PATRIMONIO PÚBLICO: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

COPIA CONTROLADA

PROBABILIDAD: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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

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

Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata.

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

CONSECUENCIA: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

PUNTO DE RIESGO: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el ***Catálogo-Listado Puntos De Riesgo Fiscal y Causas Inmediatas***[1].

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

COPIA CONTROLADA

[1] https://www.funcionpublica.gov.co/documents/28587410/41357681/Anexo_1_Cat%C3%A1logo_Listado.pdf/d8bb55ee-d121-129f-104e-7d7e7808a1db?t=1657632602969

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

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

RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente. Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

CONTROL: Medida que permite reducir o mitigar un riesgo.

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

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

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

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

INTEGRIDAD: Propiedad de exactitud y completitud.

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

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

ACTIVO: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

NIVEL DE RIESGO: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los

COPIA CONTROLADA

objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

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

TOLERANCIA DEL RIESGO: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

CAPACIDAD DE RIESGO: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

PROGRAMA DE TRANSPARENCIA Y ÉTICA PÚBLICA (PTEP): Estrategia obligatoria en entidades públicas tras la expedición de la Ley 2195 de 2022, cuya finalidad es prevenir y controlar la corrupción, promoviendo la integridad, la legalidad y el acceso a la información, mediante la gestión de riesgos, la participación ciudadana y la divulgación proactiva de datos para fortalecer la confianza y mejorar la gestión pública.

SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA - SIGRIP: esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos

RIESGOS PARA LA INTEGRIDAD: Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas

COPIA CONTROLADA

SOBORNO: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar. (A partir de ISO37001:2025)

SOBORNO ENTRANTE: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.

SOBORNO SALIENTE: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad.

FRAUDE: errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)

CONFLICTO DE INTERÉS: Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011.

CORRUPCIÓN: Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias;
y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015)

COPIA CONTROLADA

LAVADO DE ACTIVOS: el artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades [relacionadas con un delito fuente], o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito". El Lavado de Activos puede darse por: colocación, ocultamiento e integración.

DELITO FUENTE: según el artículo 323 de la Ley 599 de 2000, son delitos fuente del lavado de activos: tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, contrabando, contrabando de hidrocarburos o sus derivados, fraude aduanero o favorecimiento y facilitación del contrabando, favorecimiento de contrabando de hidrocarburos o sus derivados, en cualquiera de sus formas.

COLOCACIÓN: es la disposición del dinero proveniente de actividades delictivas. Durante esta fase inicial, el determinador o autor introduce sus fondos ilegales en actividades legales o aparentemente legales, bien a través del sistema financiero o de otros tipos de negocios o contratos, tanto nacionales como internacionales.

OCULTAMIENTO: es la separación de fondos ilícitos de su fuente mediante una serie de transacciones, cuyo fin es desdibujar la transacción ilícita original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras para disimular el rastro documentado, la fuente y la propiedad de los fondos.

INTEGRACIÓN: es dar apariencia legítima a riqueza ilícita mediante el reingreso en la economía con transacciones comerciales o personales que aparentan ser normales. Esta fase conlleva la 10 colocación de los fondos lavados de vuelta en la economía para crear una percepción de legitimidad. El lavador podría optar por invertir los fondos en bienes raíces, artículos de lujo o proyectos comerciales, entre otros.

COPIA CONTROLADA

FINANCIACIÓN DEL TERRORISMO (FP): el artículo 345 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas". La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización.

RECAUDACIÓN: consiste en la búsqueda de fuentes de financiación por las organizaciones terroristas, bien sean de origen legal, como los aportes de los Estados, individuos, entidades, organizaciones y donantes en general que apoyan su causa o son engañados, así como recursos provenientes de cualquier actividad delictiva, fondos que generalmente circulan en efectivo.

TRANSMISIÓN: es la fase intermedia que busca poner el dinero recaudado a disposición de la organización terrorista, quedando simplemente la espera de su utilización final; corresponde al movimiento de los fondos a través de distintas técnicas, se trata de ocultar sus movimientos y destino final.

UTILIZACIÓN: fase donde los fondos se utilizan básicamente para la financiación de la logística estructural de la organización o la logística operativa en materia de planeación y ejecución de actos terroristas.

FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA (FP): fondos u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización.

DEBIDA DILIGENCIA (DUE DILLIGENCE): proceso que deben llevar a cabo las entidades para identificar, prevenir, mitigar y explicar cómo abordan los impactos negativos reales y potenciales en sus propias actividades, su cadena de suministro y otras relaciones comerciales.

COPIA CONTROLADA

DEBIDA DILIGENCIA EN EL CONOCIMIENTO DE LA CONTRAPARTE (DEBIDA DILIGENCIA DEL CLIENTE): proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera.

FUNCIÓN DE CUMPLIMIENTO: función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.

CONTRAPARTE: cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización.

PARTE INTERESADA: es un tipo de contraparte con la cual no se ha establecido ninguna relación o vinculo, pero que ha manifestado formalmente su interés en establecerlo.

PARTE VINCULADA: para efectos del SIGRIP, es una contraparte dependiente de la organización con la cual se ha establecido una relación de especial de sujeción por su relación legal o reglamentaria, o laboral.

PARTE RELACIONADA: para efectos del SIGRIP, es una contraparte independiente de la organización con la cual se ha establecido una relación comercial, contractual o legal; o respecto de la cual se ejerce algún grado de control jerárquico, de tutela o de propiedad, sin detrimento de su independencia.

COPIA CONTROLADA

2. NORMATIVIDAD

Año	NORMA	NOVEDAD
1991	Constitución Política	Adopta los principios de la función administrativa y elimina el control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno.
1993	Ley 87	Crea el Sistema Institucional de Control Interno y dota a la administración de un marco para el control de las actividades estatales, directamente por las mismas autoridades.
1998	Ley 489	Fortalece el Control Interno, con la creación del Sistema Nacional de Control Interno
2001	Decreto 1537	Provee elementos técnicos y administrativos para fortalecer el Sistema de Control Interno (SCI). Establece la administración del Riesgo se contempla como parte integral del fortalecimiento de los SCI
2005	Decreto 1599	Adopta un marco general para el ejercicio del Control Interno, a través del Modelo Estándar de Control Interno –MECI y dota al Estado colombiano de una estructura única.
2012	Decreto 1599	Integra en un solo sistema todas aquellas herramientas de gestión, presenta a las entidades el Modelo Integrado de Planeación y Gestión, el cual recoge el Sistema de Desarrollo Administrativo en cinco políticas MECI se configura como la herramienta de seguimiento y control del Modelo.
2014	Decreto 943	Actualiza el MECI a una versión más moderna y de fácil comprensión por parte de las entidades.
2015	Ley 1753	Integra en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulado con los Sistemas Nacional e Institucional de Control Interno (Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998)
2017	Decreto 1499	Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades. Actualiza el Modelo Estándar de Control Interno para el Estado Colombiano – MECI a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG (correspondiendo a la 7° Dimensión de MIPG)
2020	Guía	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 Diciembre de 2020.
2022	Guía	Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - Versión 6 Noviembre 2022
2025	Guía	Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - Versión 7 Agosto 2025

COPIA CONTROLADA

3. OBJETIVO

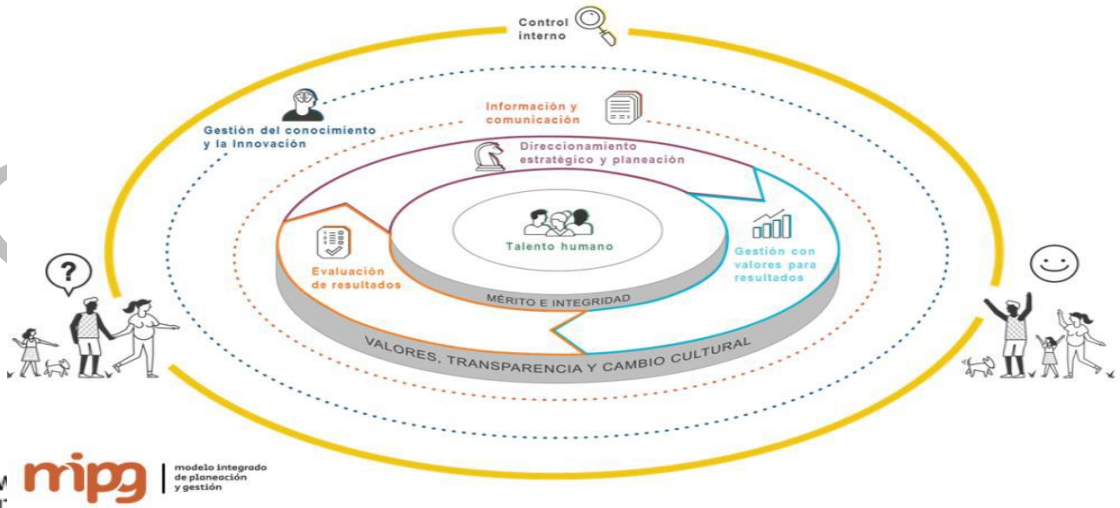
Establecer los principios básicos, lineamientos, responsabilidades y directrices que permitan disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones en que se pueda ver expuesta la administración del municipio de Cartago – Valle del Cauca, en función del desarrollo de un pensamiento basado en riesgos, aplicando las normas en materia de riesgos con el fin de alcanzar de manera eficaz y efectiva la misión y el cumplimiento de los objetivos institucionales.

4. ALCANCE

La Política Institucional de Administración del Riegos debe ser aplicada por toda la entidad desde el Direccionamiento Estratégico como línea estratégica (Alta Dirección y el Comité Institucional de Coordinación de Control Interno) hasta el nivel operativo en cumplimiento de las tareas diarias del que hacer de la administración del municipio de Cartago – Valle del Cauca. Aplica a todos los procesos y proyectos de la administración y a todas las actividades realizadas por los funcionarios durante el ejercicio de sus funciones y en representación de la Administración Municipal.

5. MARCO DE REFERENCIA

El modelo integrado de planeación y gestión (MIPG) será el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de la entidades, este modelo tiene 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.



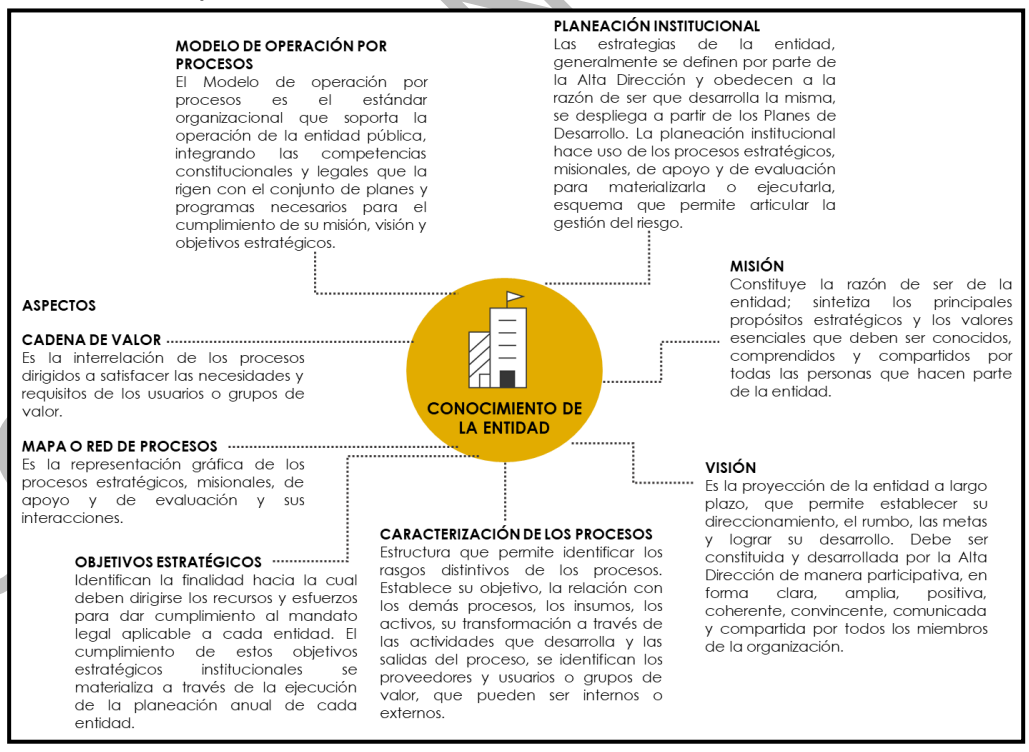
COPIA CONTROLADA

De acuerdo con el numeral 2.2.1 “política de planeación institucional” de la dimensión “Direccionamiento estratégico y planeación” del MIPG se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

En este sentido, es claro que la identificación y valoración de riesgos se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos.

Este desarrollo 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, sistemas de información, tendrá insumos esenciales para iniciar con la aplicación de la metodología propuesta para la administración del riesgo.

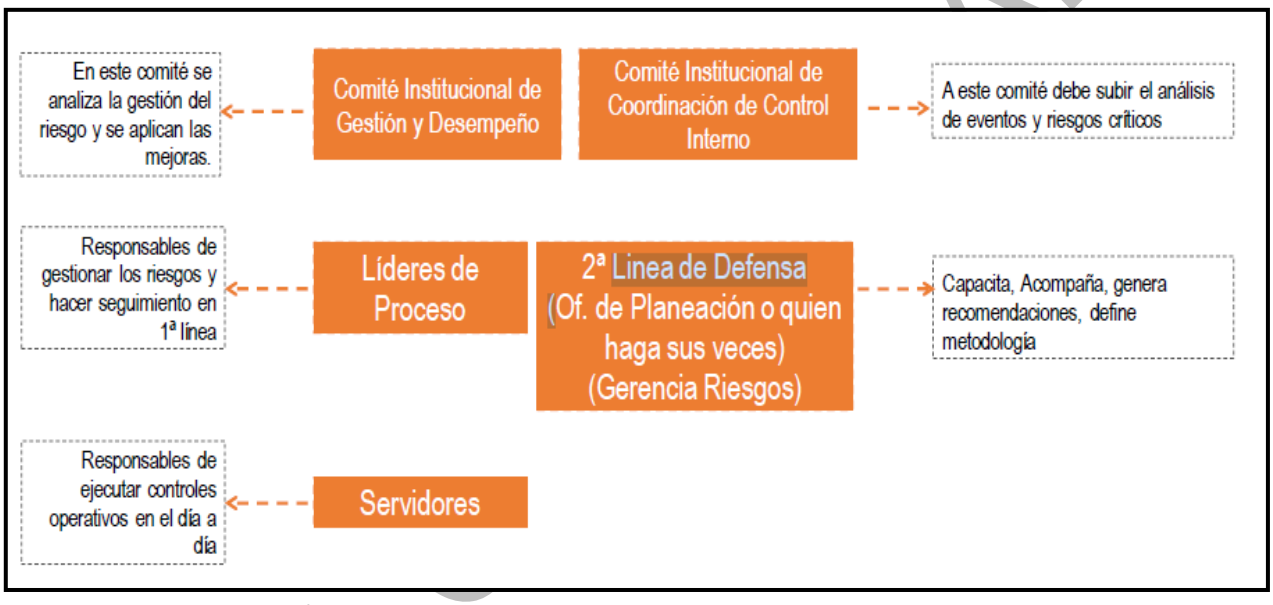
A continuación, se puede observar su interrelación:



CONTROLADA

6. INSTITUCIONALIDAD

El modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, y el Comité Institucional de Coordinación de Control Interno, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:



COPIA CONTROLADA

7. NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Planeación y Gestión (MIPG) en la dimensión siete “Control Interno” desarrolla a través de la Línea Estratégica y las tres Líneas de Defensa de responsabilidad de la gestión del riesgo y control.

LÍNEA ESTRATÉGICA	
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno	
Responsables	**Actividades de monitoreo y revisión**
Alta Dirección y Comité Institucional de Coordinación de Control Interno	• Revisar, aprobar y socializar la Política de administración del riesgo. • Aprobar el Mapa de Riesgos de Gestión, Corrupción y Riesgos de Seguridad de la Información en Comité Directivo. • Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo) • Analizar los cambios en el contexto de la organización (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles • Realizar seguimiento y análisis periódico a los riesgos institucionales

COPIA CONTROLADA

1ª. LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	
Responsables	**Actividades de monitoreo y revisión**
Responsables de los Procesos	• Identificar y valorar los riesgos de Gestión, Corrupción y de la Seguridad de la Información que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera. • Diseñar, ejecutar 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. • Establecer la(s) acción(es) asociadas al control que mitigan o reducen cada riesgo, determinando el periodo de ejecución, indicador, área responsable y registro que evidencie el cumplimiento de la acción. • Informar a la Secretaria de Planeación y Medio Ambiente (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. • Solicitar modificaciones de los diferentes tipos de riesgos de acuerdo con los autoevaluaciones, observaciones o informes de las auditorías internas o externas. • Realizar monitoreo y revisión al Mapa de Riesgos de Gestión, Corrupción y Seguridad de la Información.

COPIA CONTROLADA

2ª. LÍNEA DE DEFENSA	
Tiene a cargo responsabilidades directas frente al monitoreo y evaluación del estado de controles y la Gestión del Riesgo, asegura que la identificación, análisis, valoración, monitoreo y las actividades de control de los riesgos de Gestión, Corrupción y de Seguridad de la Información implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	
Responsables	**Actividades de monitoreo y revisión**
Secretaria de Planeación, Supervisores e interventores de contratos o proyectos, comités de contratación, áreas financieras, Tics entre otros	• Asesorar a la línea estratégica en el análisis del contexto de la organización (interno y externo), para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional y presentarlo para aprobación ante el Comité Directivo • Acompañar, orientar y entrenar a los responsables de los procesos en la identificación, análisis y valoración del riesgo • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de los procesos • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones. • Evaluar que los riesgos sean consistentes con la actual política de la entidad y que sean monitoreados por la primera línea de defensa • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno • Actualizar la versión del Mapa de Riesgos de Gestión y Corrupción o el Mapa de Riesgos de Seguridad de la Información según sea el caso, con las solicitudes de modificación aprobadas por la Alta Dirección para su respectiva publicación en la Página WEB de la Entidad.

COPIA CONTROLADA

3ª. LÍNEA DE DEFENSA	
Proporciona información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.	
Responsables	**Actividades de monitoreo y revisión**
Dirección Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Asesorar de forma coordinada con la Dirección de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. • Llevar a cabo el seguimiento a los riesgos consolidados y presentar dicho informe de seguimiento al CICCI según la programación del Plan Anual de Auditoria o reuniones de este comité • Recomendar mejoras a la política de administración del riesgo. • Verificar la inclusión de los riesgos que se materializan en el plan de mejoramiento.

8. BENEFICIOS APLICACIÓN DE LA POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DEL RIESGO

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones
- Garantizar la operación normal de la organización
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)

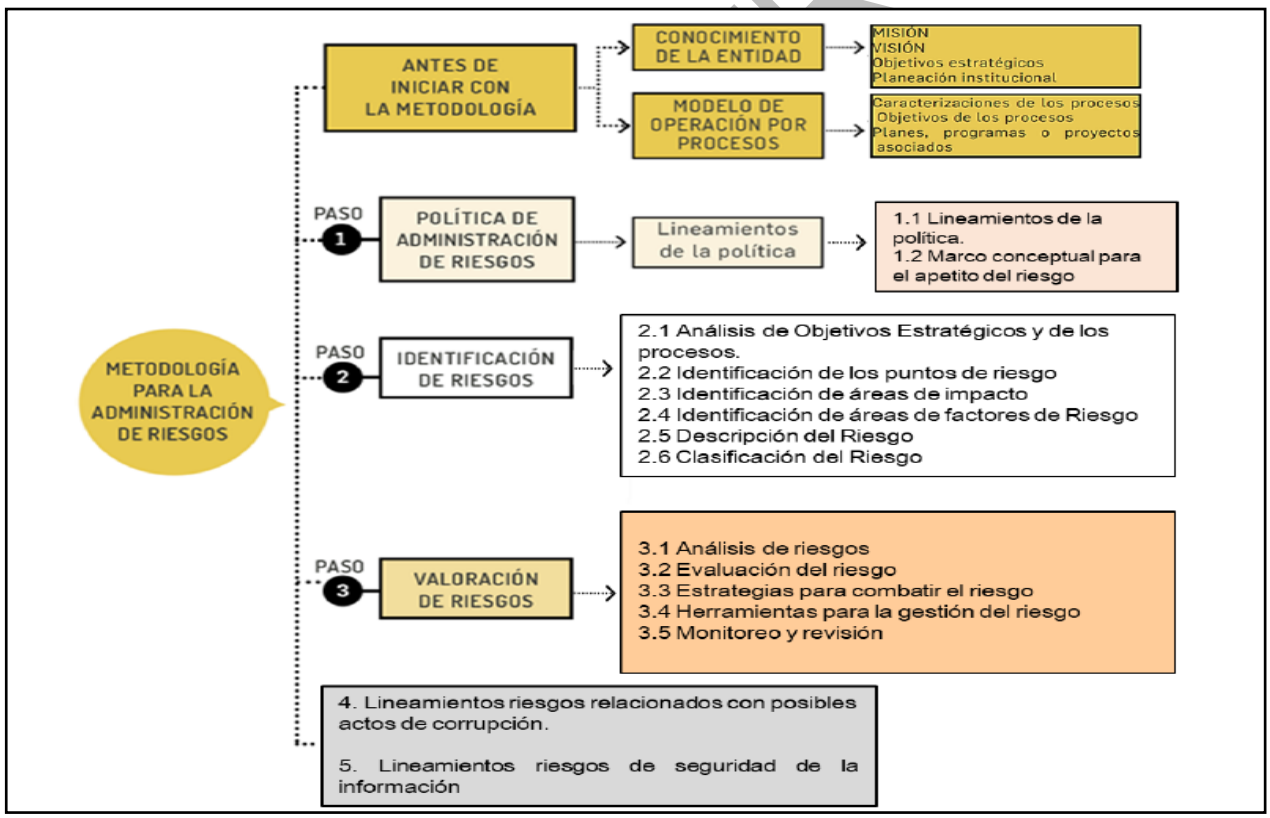
COPIA CONTROLADA

- Fortalecimiento de la cultura de control de la organización
- Incrementa la capacidad de la entidad para alcanzar sus objetivos
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

9. METODOLOGIA PARA LA ADMINISTRACION DE RIESGOS

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

Metodología para la administración de riesgos de Gestión



Tomado de: guía de administración del riesgo y el diseño de controles en entidades públicas

COPIA CONTROLADA

10. LINIEAMIENTOS DE LA POLITICA DEL RIESGO

¿QUÉ ES?

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

¿QUIÉN LA ESTABLECE?

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

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

¿QUÉ SE DEBE TENER EN CUENTA?

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

¿QUÉ DEBE CONTENER?

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

Metodología para la administración de riesgos de Gestión
Tomado de: guía de administración del riesgo y el diseño de controles en entidades públicas

El aspecto central para el desarrollo y la consolidación de la política de administración de riesgos, es la identificación y análisis del mapa de riesgos institucional y la formulación y actualización de la matriz de riesgos (matriz de calor y zonas de riesgo - Formato Matriz de Riesgo.

11. MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO

Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis en cada una de las entidades, iniciando con las siguientes definiciones:

- Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

- Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- 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 consideran que no sería posible el logro de los objetivos de la entidad.

11.1. Determinación de la Capacidad De Riesgo

La entidad debe aplicar los valores de probabilidad e impacto contenidos en esta Guía y con base en esto debe determinar, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.

b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo”.

COPIA CONTROLADA

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

11.2. Determinación del Apetito de Riesgo

Luego de determinada la capacidad de riesgo por parte de la alta dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.

Este valor se denomina “apetito de riesgo”, dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

11.3 Tolerancia de Riesgo

La tolerancia de 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.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.
El límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

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

COPIA CONTROLADA

12.IDENTIFICACION DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

12.1. Análisis de objetivos estratégicos y de los procesos:

Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

Análisis de objetivos estratégicos	Análisis de objetivos del proceso
La administración municipal debe analizar los objetivos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso Es necesario revisar que los objetivos estratégicos se encuentren alineados con Misión y la Visión institucional, si como analizar su adecuada formulación es decir que sean específicas, medibles, alcanzables, relevantes y proyectadas en el tiempo.	Los objetivos de los procesos deben estar alineados con los objetivos estratégicos, así como de su misión y visión, es decir asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.

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

COPIA CONTROLADA

12.3. Identificación Área de impacto: El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la administración municipal en caso de materializarse un riesgo. Los impactos que aplican son afectación económica o (presupuestal) y reputacional.

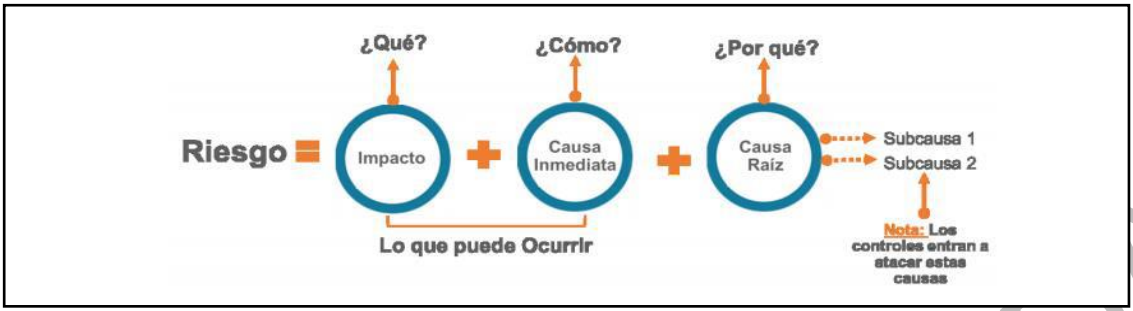
12.4. Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos.

FACTOR	DEFINICION	DESCRIPCION
PROCESOS	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
TALENTO HUMANO	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
TECNOLOGIA	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
INFRAESTRUCTURA	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
EVENTO EXTERNO	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

12.5. Descripción del Riesgo

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

COPIA CONTROLADA



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

Desglosando la estructura se obtiene:

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

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

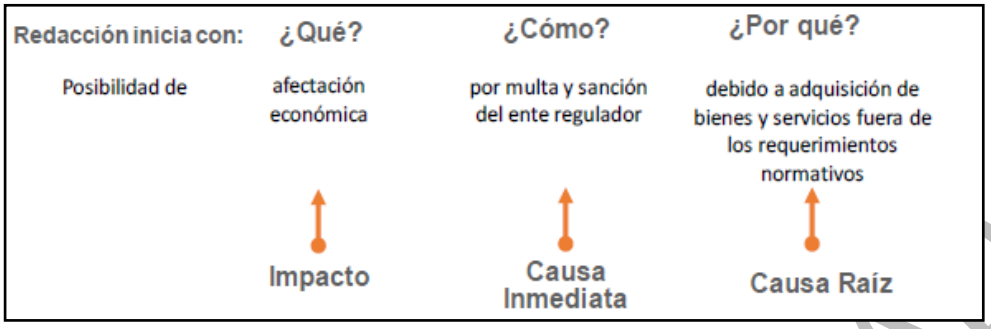
Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Ejemplo:

Proceso: gestión de recursos
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisidores) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:

COPIA CONTROLADA



Premisas para una adecuada redacción del riesgo

No describir como riesgos omisiones ni desviaciones del control.

Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

No describir causas como riesgos

Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

No describir riesgos como la negación de un control.

Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

No existen riesgos transversales, lo que pueden existir son causas transversales.

Ejemplo: pérdida de expedientes.

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

Clasificación del riesgo: Permite agrupar los riesgos identificados, los cuales se clasifican en las siguientes categorías: Ejecución y administración de procesos; Fraude externo; Fraude interno; Fallas tecnológicas; Relaciones laborales; Usuarios, productos y prácticas; Daños a activos fijos/ eventos externos.

COPIA CONTROLADA

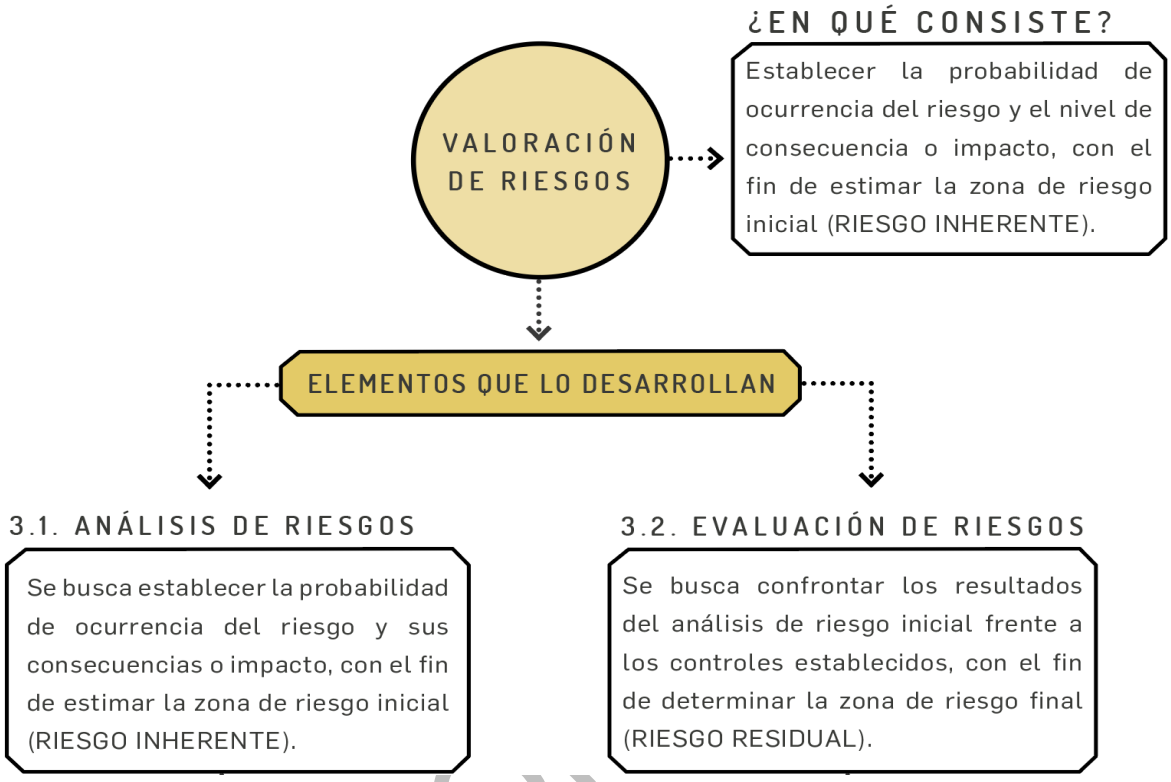
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

13. VALORACION DEL RIESGO

Establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia e impacto, con el fin de estimar la zona del riesgo inicial (RIESGO INHERENTE).

Estructura para el desarrollo de la valoración del riesgo.

COPIA CONTROLADA



13.1. Análisis De Riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

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.

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

COPIA CC

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	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

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

Determinar el impacto: para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles **se debe tomar el nivel más alto**, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

COPIA CON

Tabla de impacto: En esta tabla se definen los impactos económicos y reputacionales como las variables principales, y cuando se presenten ambos impactos para un riesgo, con diferentes niveles, se debe tomar el nivel más alto.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Ejemplo:

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

N.º de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.

COPIA CO

Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 500 SMLMV.
Aplicando las tablas de probabilidad e impacto tenemos:

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

→ La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

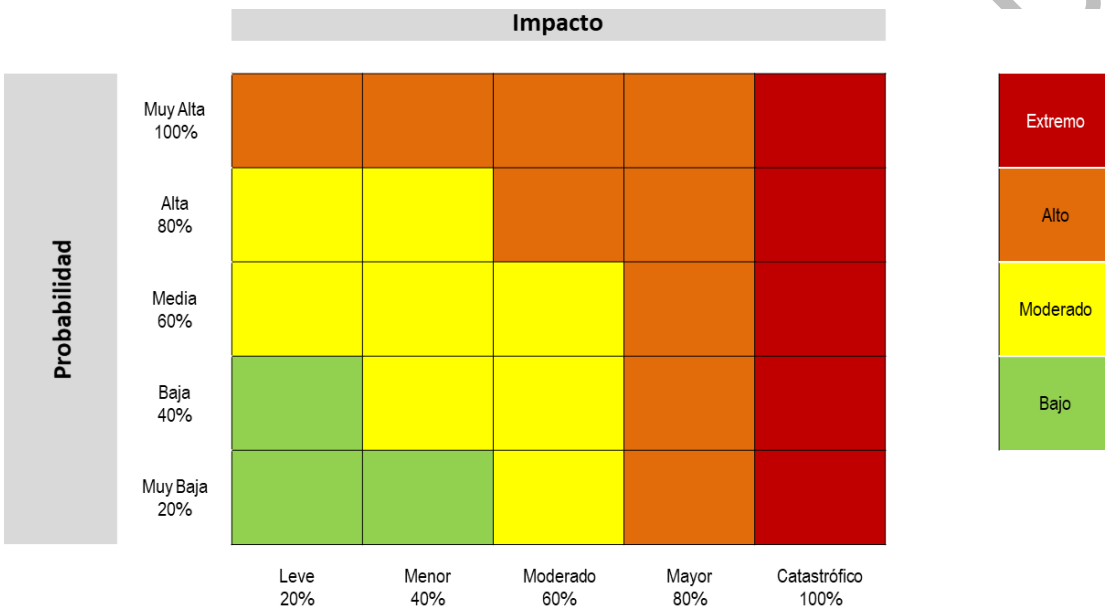
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

→ La afectación económica se calcula en 500SMLMV, el impacto del riesgo es **mayor**.

Probabilidad inherente= media 60%, **Impacto inherente:** mayor 80%

13.2. Evaluación de Riesgos: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Análisis preliminar (riesgo inherente): 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:



Ejemplo:
Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

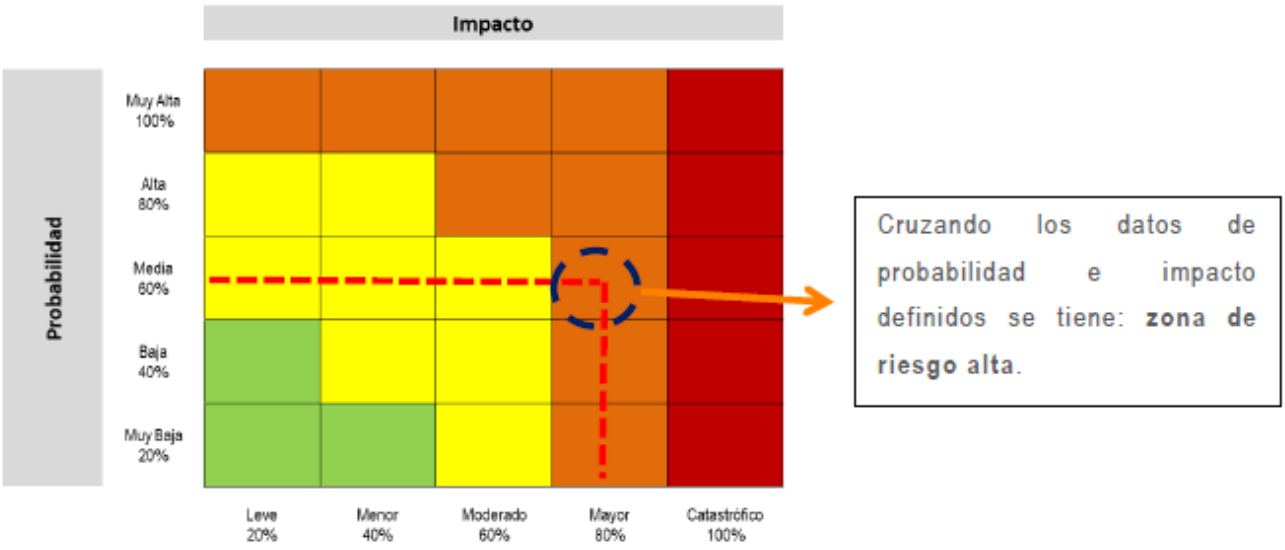
Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos

Probabilidad Inherente= moderada 60%

Impacto Inherente: mayor 80%

COPIA CONTROLADA

Aplicando la matriz de calor tenemos:



13.3 Valoración de Controles

Para la valoración de controles se debe tener en cuenta:

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso si aplica el criterio experto.

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo

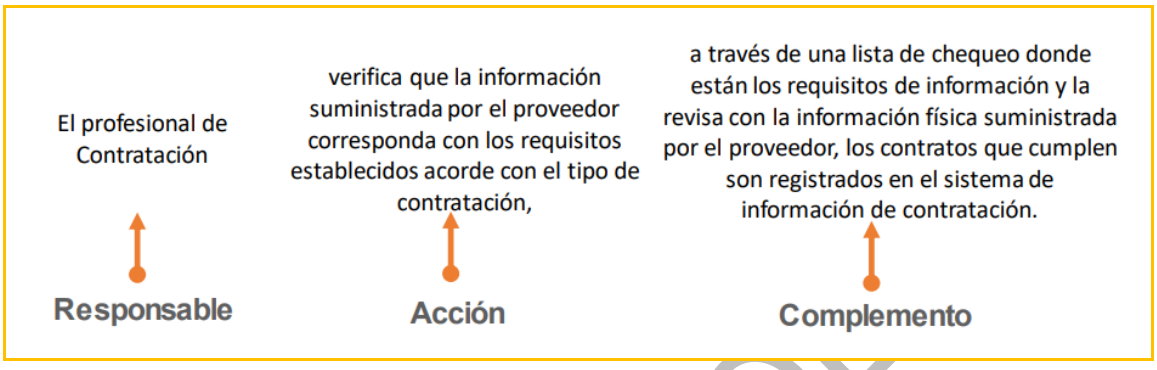
13.3.1 Estructura para la descripción del control: Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

- Acción: Se determina mediante verbos que indican la acción que deben realizar como parte del control.

COPIA CONTROLADA

- Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control.



13.4. Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión.

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

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

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

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

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

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

COPIA CONTROL

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

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

COPIA CONTROLADA

13.6. Nivel de Riesgo (Riesgo Residual): el 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 (Ver. Guía para la administración de riesgos y el diseño de controles en entidades públicas V.6 Apartado 3.2.3.[2])

13.7. Estrategias para combatir el riesgo: decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

Opción para el manejo del riesgo	Descripción
Evitar el riesgo	Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
Compartir el riesgo	Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo. Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.
Reducir el riesgo	El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este. Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

COPIA CONTROLADA

[2] https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238

Aceptar el riesgo	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Importante: Ningún riesgo de corrupción debe ser aceptado.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

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

13.8. Herramientas para la gestión del riesgo: como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

Gestión de eventos: un evento es un riesgo materializado, 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 de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia

14. LINEAMIENTOS PARA EL TRATAMIENTO DE RIESGOS FISCALES

14.1. Control fiscal interno y prevención del riesgo fiscal: este tipo de control tiene como finalidad prevenir la constitución de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. A partir de lo anterior, el control fiscal además de posterior y selectivo a través de las

COPIA CONTROLADA

auditorías (control micro), es preventivo y concomitante, buscando 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 como:

- **Control fiscal Multinivel**: Es 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.

- **Control fiscal Interno (CFI):** Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y 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 defensa, 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.

14.2. Definición y elementos del riesgo fiscal: se define riesgo fiscal como el efecto dañoso sobre recursos públicos o bienes 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: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

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

Lo anterior se puede resumir de la siguiente manera:

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

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

COPIA CONTROLADA

14.3. Metodología y paso a paso 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, que es fundamental para el resultado de la gestión de cada entidad y para la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros).

Paso 1: Identificación de riesgos fiscales.

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

Paso2: 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. 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.

Paso 3. 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.

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.

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

COPIA CONTROLADA

deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Ejemplo:

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 gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

¿Cuál es el daño? El daño fiscal corresponde al monto pagado por concepto de intereses moratorios

¿Cuál es el hecho generador? La omisión de pagó oportuno del canon de arrendamiento.

Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

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 identificados como resultado del estudio de fallos de Contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta:

- Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.

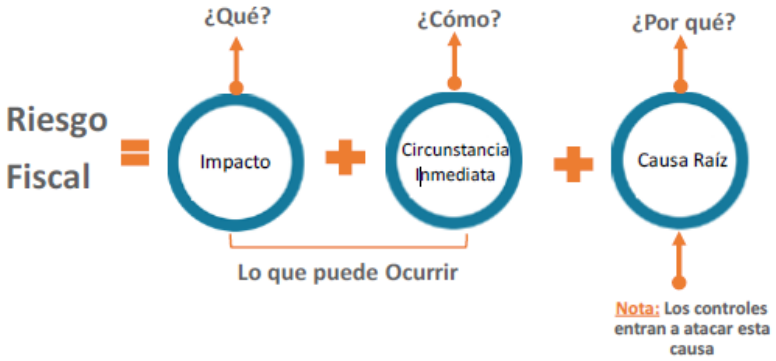
- Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

- Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica - causa raíz- para que se presente el riesgo.

COPIA CONTROLADA

- Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

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



Ejemplo:

Proceso: Gestión de Recursos

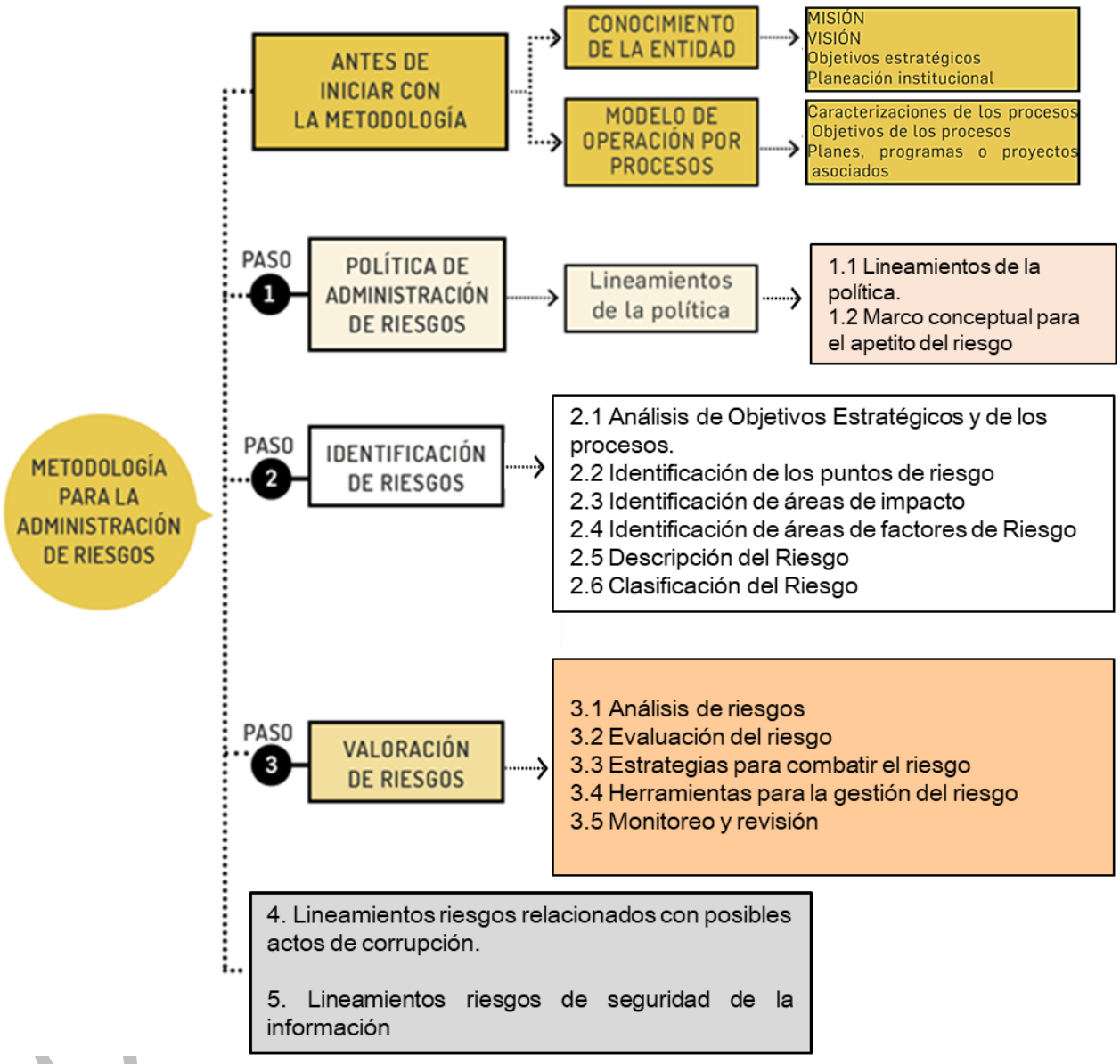
Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

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.

En lo que respecta a la Valoración del Riesgo, determinación de Riesgo Inherente, la Valoración de Controles y Nivel de Riesgo Residual, se aplican las pautas estipuladas al momento de diligenciar la Herramienta Matriz de Riesgo, adoptada por parte de la Administración Municipal.

COPIA CONTROLADA

15. TRATAMIENTO RIESGOS DE CORRUPCIÓN



Teniendo en cuenta que el Gobierno Nacional viene impulsando y desarrollando diferentes políticas públicas con miras a disminuir los niveles de corrupción en todos los ámbitos, la Secretaría de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011 diseñó una metodología para que todas las entidades determinen su Plan Anticorrupción y de Atención al ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción. Entendiendo que los riesgos de corrupción se convierten en una tipología de riesgos que debe ser controlada por la entidad, éstos deben incorporarse en primera instancia en el mapa de riesgos del proceso, sobre el cual se han identificado, de modo tal que el responsable o líder del mismo pueda realizar el seguimiento correspondiente, en conjunto con los riesgos de gestión propios del proceso, lo que promueve que el responsable tenga una mirada integral de todos los riesgos que pueden llegar a afectar el desarrollo de su proceso.

Generalidades:

Teniendo en cuenta las definiciones dadas frente a la corrupción, la guía para la administración del riesgo define:

- Los hechos de corrupción son inaceptables e indeseables.
- El riesgo de corrupción debería tratar de evitarse, estableciendo controles para el hecho de corrupción.
- Elaboración: el mapa de riesgos de corrupción lo elabora anualmente cada líder de proceso junto con su equipo de trabajo.
- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014. En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la

COPIA CONTROLADA

publicación.

- Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito los líderes de los procesos diseñarán las actividades o mecanismos necesarios de socialización el mapa actualizado para cada vigencia con el propósito de que funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción. Así mismo, se adelantarán las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción, dejando la evidencia del proceso de socialización y publicación de sus resultados.

- Ajustes y modificaciones: Después de su publicación y durante el respectivo año de vigencia, los líderes de proceso podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el Mapa de Riesgos de Corrupción realizando la solicitud correspondiente ante la Secretaria de Planeación, Medio Ambiente y Desarrollo Económico. En este caso, deberán dejar por escrito los ajustes, modificaciones o inclusiones realizadas.

- Monitoreo: en concordancia con la cultura del autocontrol al interior de la Alcaldía Municipal de Cartago, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de gestión y de corrupción, y enviarán el monitoreo a la Oficina de Control Interno con la periodicidad definida en por parte de estos para cada vigencia.

- Seguimiento: La Oficina de control interno realizará el seguimiento a la gestión de riesgos de corrupción. En este sentido, incluirá en sus procesos de auditoría interna, el análisis de las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

COPIA CONTROLADA

15.1. Zona de riego y tratamiento

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgo de corrupción	Muy baja, baja o Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad bimestral de monitoreo para evitar a toda costa su materialización por parte de los procesos.
	Alta y extrema	Se adoptan medidas para: **REDUCIR** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. **EVITAR** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
		TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo.

15.2. Directrices de redacción para riesgos de corrupción.

El riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos.

COPIA CONTROLADA

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

Los riesgos de corrupción se establecen sobre procesos.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere revisar el ***apartado 5. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción*** de la *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, V6.*

15.3. Valoración de Riesgos de Corrupción

15.3.1. Análisis de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Criterios para calificar la probabilidad:

COPIA CONTROLADA

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

15.3.2. Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo Criterios para calificar el impacto en riesgos de corrupción.

COPIA CONTR

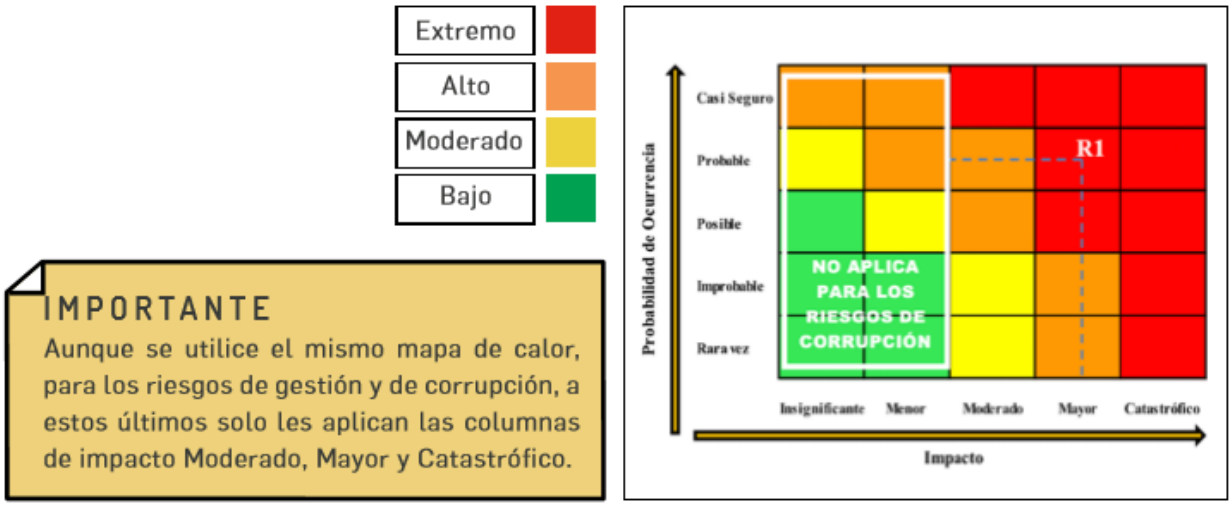
N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

15.3.3. Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

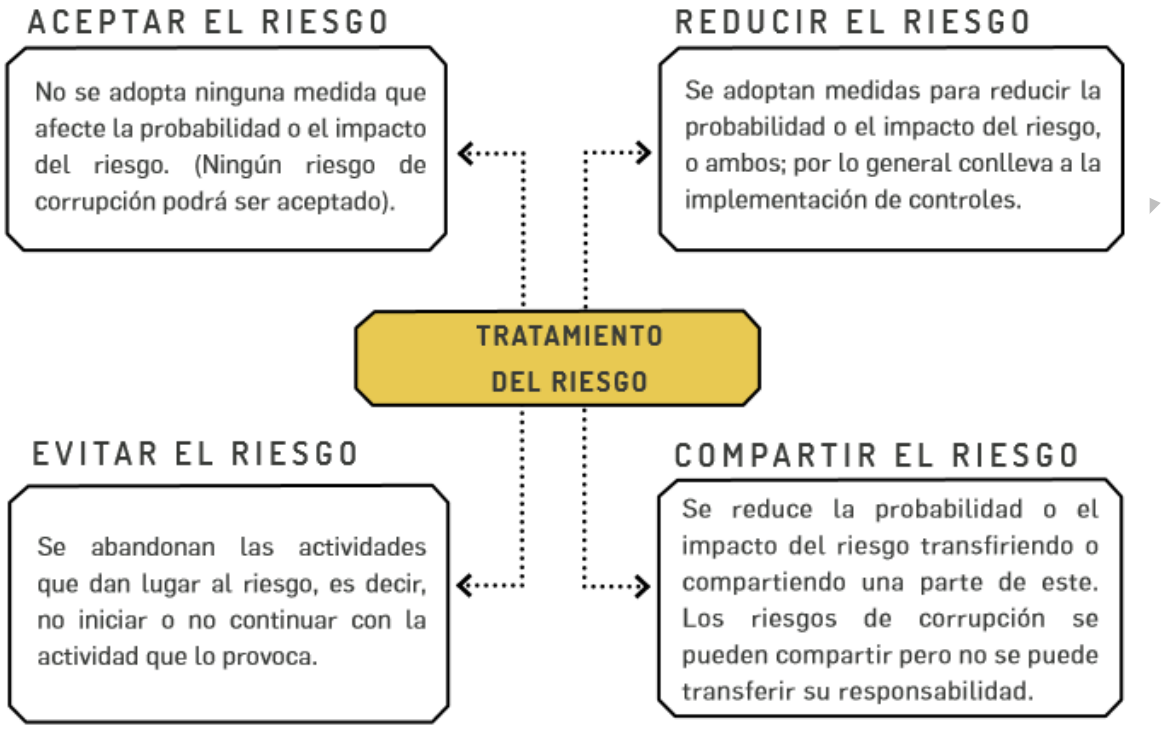
Por último ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.



15.3.4. Tratamiento del riesgo

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

COPIA CONTROLADA



Metodología para la administración de riesgos de Gestión
Tomado de: guía de administración del riesgo y el diseño de controles en entidades públicas

15.3.5. Monitoreo de riesgos de corrupción

Los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la Secretaria de Planeación, Medio Ambiente y Desarrollo Económico adelantar el monitoreo (segunda línea de defensa).

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar. Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

COPIA CON

15.3.6. Reporte de la gestión del riesgo de corrupción

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado

15.3.7. Seguimiento de riesgos de corrupción

Seguimiento: El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

15.3.8. Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.

COPIA CONTROLADA

4) Llevar a cabo un monitoreo permanente.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

16. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

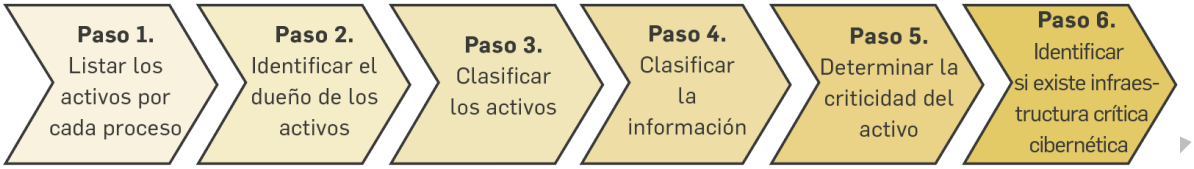
En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital, seguridad de la información, arquitectura, servicios ciudadanos digitales.

Identificación de los activos de seguridad de la información: como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: • Aplicaciones de la organización • Servicios web • Redes • Información física o digital • Tecnologías de información TI • Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

COPIA CONTROLADA

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



a. Identificación del riesgo: se podrán identificar los siguientes tres riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el ***Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas***.[3]

COPIA CONTROLADA

[3] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237907_maestro_mspi.pdf

17. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA - SIGRIP

Con la entrada en vigencia de la Ley 2195 de 2022, las entidades públicas están obligadas a implementar acciones para prevenir, gestionar y administrar los riesgos relacionados con el lavado de activos, la financiación del terrorismo, la proliferación de armas y la corrupción. Esto incluye reportar operaciones sospechosas a la UIAF, consultar listas restrictivas y aplicar las medidas que establezca el Gobierno nacional (artículo 31). En este contexto, la Secretaría de Transparencia de la Presidencia de la República recomienda que las entidades que deben adoptar un Programa de Transparencia y Ética Pública cuenten con un sistema de gestión que permita identificar, prevenir y corregir de manera integral los riesgos que afecten la integridad del servicio público o de las instituciones del Estado. Con ese propósito, se diseñó el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), que se presenta a continuación.

17.1. Integridad Pública

Las organizaciones suelen enfrentarse a situaciones en las que sus objetivos no se alcanzan debido a los distintos intereses que intervienen en la toma de decisiones, especialmente cuando se priorizan intereses individuales sobre el interés general de la entidad. En el sector público, el interés general —que corresponde a la búsqueda de los fines del Estado— también puede verse afectado por intereses particulares, lo que finalmente limita la capacidad de las entidades públicas para cumplir con las funciones que les han sido asignadas.

En este escenario, cobra una importancia central el concepto de integridad en la gestión pública. Hablar de integridad implica abordar también nociones como la moral y la ética. La moral pertenece al ámbito íntimo de cada persona y, por tanto, no puede ser regulada; mientras que la ética se relaciona con la capacidad de las personas para actuar conforme a las expectativas sociales. La integridad, a su vez, supone que un individuo, desde un comportamiento ético, se ajuste a códigos de conducta previamente establecidos. Así, aun cuando en una organización existan diversas perspectivas éticas, es posible fomentar una cultura de integridad entre sus colaboradores.

En el sector público, se espera que los servidores y colaboradores actúen dentro de un marco ético que les permita anteponer el interés general del Estado en todas las decisiones derivadas de sus funciones o servicios. Existen múltiples

COPIA CONTROLADA

normas que definen este comportamiento esperado y, conforme a la Constitución Política de Colombia, los servidores son responsables tanto por sus actos como por sus omisiones. En consecuencia, cualquier decisión que no priorice el interés general constituye un incumplimiento de la conducta esperada y un riesgo para la integridad institucional.

En conclusión, las entidades públicas deben garantizar el fortalecimiento de una cultura de cumplimiento que, reconociendo la individualidad y la ética personal de cada colaborador, promueva actuaciones íntegras basadas en el respeto a la ley. No obstante, además de esta cultura orientada a la legalidad, es indispensable adoptar medidas que permitan gestionar las incertidumbres que puedan afectar la protección del interés general, como se plantea en el capítulo siguiente.

17.2. Amenazas Para La Integridad Pública

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

17.2.1. Soborno

El soborno puede definirse como la acción de ofrecer, prometer, entregar, aceptar o pedir un beneficio indebido, de cualquier tipo o valor —ya sea económico o no—, de manera directa o indirecta, y sin importar el lugar donde ocurra, con el fin de influir en que una persona realice o deje de realizar una determinada acción, infringiendo la legislación aplicable. Este fenómeno puede presentarse en dos modalidades: soborno entrante, cuando un servidor de la entidad recibe el ofrecimiento indebido, y soborno saliente, cuando son los propios servidores quienes ofrecen dicho beneficio a terceros en nombre de la entidad.

En el Código Penal Colombiano, el soborno se encuentra regulado a través de las figuras de cohecho propio, cohecho impropio y cohecho por dar u ofrecer, todas ellas clasificadas como delitos contra la administración pública y

COPIA CONTROLADA

consideradas formas de soborno. En el ámbito entre particulares, el Código Penal solo contempla una tipificación general del delito de soborno.

17.2.2. Fraude

El fraude se refiere a errores, omisiones, reportes falsos o descripciones incorrectas realizados de manera intencional o por negligencia, con el propósito de obtener un beneficio propio o para terceros. Este puede ser interno, cuando involucra a colaboradores de la organización, o externo, cuando es cometido por personas ajenas a la entidad y esta resulta afectada.

El fraude externo constituye un riesgo de naturaleza operativa, derivado de acciones realizadas por terceros, por lo que se considera principalmente un riesgo general asociado a la gestión de la entidad.

17.2.3. Inadecuada Gestión del Conflicto de Intereses

Un conflicto de intereses se presenta cuando un servidor público debe tomar decisiones sobre un asunto en el cual él mismo tiene un interés particular y directo, o cuando dicho interés recae en su cónyuge, pareja permanente, familiares hasta el cuarto grado de consanguinidad, segundo de afinidad o primero civil, o en sus socios, ya sean de hecho o de derecho. En otras palabras, ocurre cuando el interés general, propio del ejercicio público, entra en oposición con un interés personal y directo del servidor.

Aunque la existencia del conflicto de intereses no constituye por sí misma una falta, sí están previstos en los códigos de conducta diversos comportamientos que regulan su declaración y manejo adecuado. La normativa nacional establece que cualquier servidor que tenga un interés particular en un asunto público debe abstenerse de participar en la decisión, pues se considera legalmente impedido.

17.2.4. 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

COPIA CONTROLADA

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"

17.2.5. 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.

17.3. SISTEMA DE GESTIÓN DEL RIESGO

Dadas las diversas amenazas que pueden afectar la integridad pública y generar riesgos o perjuicios, es fundamental que las organizaciones, desde un enfoque basado en riesgos, gestionen los eventos que podrían presentarse en su interior. Esta gestión requiere que las entidades identifiquen, analicen y evalúen los riesgos, reconociendo la existencia de situaciones que pueden convertirse en factores que los potencien.

En esta perspectiva, las entidades deben contar con un sistema que articule reintegre distintos componentes para garantizar una gestión integral del riesgo. Por ello, es necesario que adopten un Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).

El SIGRIP busca conectar la Política de Gestión Integral de Riesgos que formule cada entidad —que incluye la administración de los riesgos generales de la gestión, los riesgos fiscales de carácter preventivo y los riesgos de seguridad de la información—

COPIA CONTROLADA

con otros elementos indispensables para gestionar adecuadamente los riesgos que afectan la integridad pública. En última instancia, un riesgo operativo, fiscal o de seguridad de la información puede originarse en hechos como el soborno, el fraude, un conflicto de intereses mal manejado o actos de corrupción. Asimismo, estos pueden facilitar actividades como el lavado de activos, la financiación del terrorismo o la proliferación de armas de destrucción masiva. Por ello, es indispensable abordar los riesgos para la integridad pública de manera integral y en coordinación estrecha con la gestión institucional del riesgo.

El SIGRIP establece que la entidad debe implementar diversos instrumentos para la gestión del riesgo, actuar con diligencia en el conocimiento de sus contrapartes e incorporar una función de cumplimiento en sus procesos. Todo esto se suma a la identificación y valoración de los riesgos conforme a la metodología definida en la Política de Gestión Integral de Riesgos adoptada. La interacción de estos componentes asegura que la gestión pública se desarrolle con integridad, es decir, en estricto cumplimiento de la ley en toda la actividad 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.

17.3.1. 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.

COPIA CONTROLADA

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.

COPIA CONTROLADA

h. 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.

17.3.2. Liderazgo del Sistema

De acuerdo con lo señalado en esta Guía, las entidades que participen en la formulación de la Política para la Gestión Integral de Riesgos deben establecer distintos niveles de responsabilidad (ver numeral 2.3.4). Asimismo, en la sección 1.2 se explica que la gestión del riesgo requiere la participación de toda la organización y se vincula con las diferentes líneas de aseguramiento previstas en el Modelo Estándar de Control Interno. En el caso del SIGRIP, es necesario incorporar ciertos roles y responsabilidades adicionales dentro de esos niveles de responsabilidad. Estos se articulan según el esquema de líneas y los roles definidos en los Programas de Transparencia y Ética Pública, y se resumen en la Tabla 31 que se presenta a continuación.

Linea Estratégica	3ra Linea	2da Linea	1ra Linea
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.

COPIA CONTROLADA

17.3.3. Planificación

Conforme a lo dispuesto en esta Guía, las entidades que formulen la Política para la Gestión Integral de Riesgos deben definir un objetivo (ver numeral 2.3.1) y un alcance (ver numeral 2.3.2), así como establecer el marco de apetito de riesgo (ver numeral 2.4) y la metodología que emplearán (ver numeral 2.3.5). Para ello, deberán considerar los siguientes elementos clave del SIGRIP:

✓ El objetivo debe incluir explícitamente la protección de la integridad pública, reconociendo que la gestión institucional de riesgos busca garantizar que la entidad actúe en coherencia con los códigos vigentes y pueda enfrentar adecuadamente las amenazas que afectan un relacionamiento íntegro con el Estado.

✓ El alcance de la Política debe incorporar los aspectos relevantes de la organización identificados en el análisis del contexto interno y externo, como: los distintos grupos de valor con los que interactúa la entidad, en especial sus contrapartes; las entidades bajo su control y aquellas que ejercen control sobre ella; los procesos, servicios, trámites u otras operaciones administrativas sobre todo aquellas que implican interacción y las jurisdicciones o territorios donde desarrolla sus actividades.

17.3.4. Apoyo

Para que el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) funcione de manera adecuada, la entidad debe contar con los recursos necesarios, definir con precisión los atributos comportamentales requeridos, implementar una estrategia de formación y comunicación, y documentar todas las actividades realizadas. En este sentido:

✓ La entidad debe identificar los recursos financieros y humanos disponibles, las soluciones tecnológicas, las habilidades especializadas, la infraestructura organizacional, el material de referencia y la experiencia con la que cuenta. Todos estos recursos deben quedar claramente registrados tanto en la Política para la Gestión Integral de Riesgos como en cada componente del SIGRIP. Este ejercicio también permite detectar necesidades de desarrollo y formación profesional que contribuyan a fortalecer el Sistema.

COPIA CONTROLADA

✓ La Política para la Gestión Integral de Riesgos debe definir las características que deben cumplir las personas cuyo trabajo incida en el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), incluyendo su desempeño y las operaciones que ejecutan. En particular, se debe asegurar que quienes estén a cargo de la Administración del Programa de Transparencia —y, por extensión, de la administración del SIGRIP— cuenten con las competencias necesarias, es decir, con la educación, formación y experiencia adecuadas.

- ✓ La entidad debe garantizar que todo el personal —incluidos los líderes, el administrador, la Alta Dirección y, en general, toda la organización— comprenda y tome conciencia del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP). Para ello, la acción de Formación del Programa de Transparencia y Ética Pública debe incorporar contenidos relacionados con:

  - Los objetivos y el alcance del Sistema.
  - Cada uno de sus elementos.
  - Los beneficios que el Sistema aporta a la organización.
  - Las consecuencias de no cumplir con sus requisitos.

✓ La toma de conciencia sobre el SIGRIP también supone comunicar, tanto interna como externamente, los resultados de su funcionamiento y cualquier actualización del Sistema o de sus componentes. Por ello, la acción de Comunicación del Programa de Transparencia y Ética Pública debe incluir lineamientos sobre la forma y periodicidad con la que se divulgarán dichos resultados y modificaciones.

✓ Cada componente del Sistema debe estar debidamente documentado. Por lo tanto, una vez implementado, se deben adelantar las gestiones necesarias para incorporar al Sistema de Gestión los documentos del SIGRIP, así como incluirlos en la gestión archivística institucional. Para ello, la entidad podrá crear y actualizar información documentada, controlar su administración y garantizar la protección de los datos personales y la confidencialidad cuando se trate de información clasificada o reservada. En cada elemento del Sistema deberá evaluarse de manera particular el tratamiento que se dará a dicha información.

COPIA CONTROLADA

17.3.5. Operación

Como se mencionó anteriormente, el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) está compuesto por diversos elementos que funcionan e interactúan de manera articulada. Su componente central es la Política para la Gestión Integral de Riesgos, que cada entidad debe elaborar junto con el correspondiente mapa de riesgos. Esta Política establece los mecanismos para identificar y valorar los riesgos a los que se enfrenta la organización, incluidos aquellos que afectan la integridad pública. No obstante, por sí sola no es suficiente para gestionar de forma completa riesgos como el soborno, el fraude, la inadecuada gestión de conflictos de intereses, la corrupción y los relacionados con LA/FT/FP. Por ello, para lograr una gestión verdaderamente integral, se incorporan tres elementos adicionales 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 Sistema se presenta en la figura a continuación:

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.

17.3.5.1. 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 deben identificar y valorar los riesgos que puedan afectar el ejercicio íntegro de la función pública, incluidos los riesgos de LA/FT/FP. Aunque la corrupción constituye la principal amenaza a la integridad, existen manifestaciones específicas —como el soborno, el fraude y la inadecuada gestión del conflicto de intereses— que deben ser reconocidas y evaluadas de manera individual. Asimismo, es necesario gestionar los riesgos asociados a conductas que facilitan o favorecen el lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, dado que la integridad del Estado se ve comprometida cuando sus instituciones son utilizadas para legitimar activos ilícitos o canalizar recursos hacia actividades terroristas.

No obstante, desde una perspectiva integral, los riesgos para la integridad pública deben gestionarse conjuntamente con los riesgos generales de gestión, la gestión preventiva del riesgo fiscal y los riesgos de seguridad de la información. En consecuencia, las entidades deben contar con una única Política para la gestión de todos sus riesgos.

La existencia de una sola Política implica la aplicación de una metodología común. Esto significa que los riesgos para la integridad pública pueden identificarse y valorarse mediante la metodología propuesta en el Capítulo 3 de esta Guía. Lo anterior no impide que las entidades complementen o desarrollen la metodología, siempre que los ajustes sean compatibles y no disminuyan los estándares aquí establecidos. Esta Guía fija los requisitos mínimos, pero permite adecuaciones derivadas de la autonomía institucional de las entidades públicas.

En este sentido, la entidad deberá formular una única Política para la Gestión Integral de Riesgos, la cual formará parte del SIGRIP y deberá incorporar, respecto de los riesgos para la integridad pública, las siguientes particularidades:

COPIA CONTROLADA

Paso: 1 Identificación y descripción del riesgo

1. **Respecto de la "Identificación de los puntos de riesgo.**

   En la gestión del riesgo de LA/FT/FP es fundamental considerar que los puntos de riesgo corresponden a las operaciones que realiza la entidad. Esto incluye actividades dentro del flujo de los procesos que implican un intercambio de recursos, ya sea cuando la entidad adquiere un bien o servicio y paga por él, o cuando entrega un bien o servicio por el cual recibe un pago. Estas operaciones constituyen los puntos de riesgo relevantes que deben analizarse para identificar posibles escenarios de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

   En cambio, para el riesgo de corrupción y sus manifestaciones específicas soborno, fraude y la inadecuada gestión del conflicto de intereses los puntos de riesgo pueden encontrarse en cualquier actividad del proceso, y no solamente en las operaciones que implican intercambio de recursos.

2. **Respecto de la "Identificación de áreas de impacto"**

   En el contexto de la gestión de riesgos para la integridad pública, además de los impactos económicos y reputacionales, también pueden presentarse consecuencias legales y efectos de contagio. Las consecuencias legales se refieren al incumplimiento de normas u obligaciones que puede derivar en sanciones, procesos judiciales o administrativos, así como en indemnizaciones por daños. Estas consecuencias surgen desde el momento en que una contraparte se ve involucrada en procedimientos sancionatorios o en actuaciones orientadas a declarar un incumplimiento.

   Por su parte, el contagio alude a la posibilidad de que la entidad resulte afectada en términos económicos, reputacionales o legales por las acciones de otra entidad o individuo con los que mantiene algún tipo de relación. Este efecto se manifiesta cuando un riesgo para la integridad pública se materializa en partes relacionadas, aunque no directamente vinculadas, y tiene el potencial de impactar a la entidad.

COPIA CONTROLADA

Para determinar el impacto del riesgo, las consecuencias legales y de contagio deben evaluarse considerando su afectación económica, de conformidad con lo indicado en la presente política para determinar el impacto con el fin de aplicar lo estipulado en Tabla Criterios de Impacto.

Se entiende que un riesgo se ha materializado cuando la situación previamente identificada como posible ocurre efectivamente y genera un impacto negativo en los objetivos institucionales. En el ámbito de los riesgos para la integridad pública, la materialización se evidencia siempre que exista una afectación a la reputación, a la operación, al cumplimiento o a la adecuada ejecución de los recursos.

La **consecuencia reputacional** se presenta, por ejemplo, cuando la organización aparece involucrada en denuncias o reportajes que la asocian con prácticas poco íntegras, incumplimientos normativos o actos de corrupción. La consecuencia operativa surge cuando conductas contrarias a la integridad afectan el normal desarrollo de los procesos institucionales. La consecuencia legal comienza en el momento en que una parte vinculada es incluida en procedimientos que puedan derivar en una sanción, mientras que el contagio se produce cuando quien resulta involucrada es una parte relacionada. Finalmente, la consecuencia económica puede generarse incluso desde el momento en que se presentan retrasos en la ejecución de los recursos debido a comportamientos carentes de integridad por parte del ejecutor.

Dado que la gestión del riesgo de LA/FT/FP se orienta a prevenir que la entidad sea utilizada para dar apariencia de legalidad a activos de origen delictivo o para canalizar recursos hacia actividades terroristas, toda operación sospechosa —incluso si solo se intenta— debe ser reportada, aun cuando no se hayan producido consecuencias ni se haya materializado el delito de lavado de activos.

Es importante no confundir la materialización del riesgo con la comisión de un delito, una falta o una conducta que genere responsabilidad fiscal. El riesgo puede considerarse materializado cuando existe un impacto negativo para la entidad, incluso antes de la vinculación formal a procesos sancionatorios, y también puede materializarse aunque la persona involucrada resulte posteriormente absuelta. Por ello, los riesgos para la integridad no deben interpretarse como tipos penales o disciplinarios, ni la materialización del riesgo implica un prejuzgamiento.

COPIA CONTROLADA

La gestión del riesgo tiene como objetivos fundamentales identificar, medir, controlar y monitorear los riesgos, con el fin de prevenirlos, detectarlos y corregirlos. En ningún caso este proceso debe derivar en juicios de responsabilidad ni en la imposición de sanciones. Cuando un riesgo se materializa, la respuesta institucional debe centrarse en garantizar la continuidad del negocio, es decir, en asegurar que, pese al impacto generado en los objetivos, estos puedan seguir cumpliéndose. En este sentido, la Política para la Gestión Integral de Riesgos debe orientarse a mantener la continuidad del servicio y/o el funcionamiento normal de la organización en cualquier escenario de materialización de riesgos para la integridad, independientemente de las actuaciones que correspondan a otras autoridades por razón de su competencia y aun antes de que existan decisiones de fondo sobre responsabilidades.

3. **Respecto de la "Identificación de factores de riesgo"**

Los factores de riesgo LA/FT/FP comprenden las contrapartes, los productos, los canales y las jurisdicciones. Estos constituyen los elementos mínimos que deben considerarse en cualquier análisis y, en conjunto, configuran el concepto de "transacción" u "operación". Esto implica que toda transacción es realizada por un cliente o usuario que accede o entrega un bien o servicio a la entidad, utilizando los canales disponibles y dentro de una jurisdicción determinada. La adecuada comprensión de estos factores permite a la entidad fortalecer el conocimiento de sus contrapartes, diseñar y aplicar señales de alerta, identificar operaciones inusuales y determinar y reportar operaciones sospechosas.

A partir de lo anterior, surge la necesidad de segmentar los factores de riesgo, lo que permite profundizar tanto en el conocimiento de las contrapartes como en el entendimiento de los factores con los que se relacionan.

El propósito y los beneficios de segmentar los factores de riesgo radican en identificar grupos con características y comportamientos similares, garantizando la homogeneidad dentro de cada segmento y la heterogeneidad entre ellos, conforme al análisis técnico de las variables de información. Al lograr esta diferenciación, cada segmento permite establecer de manera implícita parámetros normales de comportamiento transaccional para sus integrantes. Estos parámetros funcionan como límites de operación o señales

COPIA CONTROLADA

de alerta que facilitan identificar operaciones que se apartan de la normalidad y que pueden ser clasificadas como inusuales, lo cual activa su análisis por parte de la función de cumplimiento y, de ser necesario, su reporte oportuno a las autoridades competentes.

En este sentido, las entidades deben incorporar en la Política para la Gestión Integral de Riesgos la obligación de conservar los documentos y registros de las contrapartes y sus operaciones durante el plazo previsto en el artículo 12 de la Ley 2195 de 2022, así como asignar los recursos técnicos, tecnológicos y humanos necesarios para la adecuada gestión de estos riesgos. La Política debe, además, describir la segmentación de los factores de riesgo LA/FT/FP derivada del análisis de contexto.

4. Respecto de la "Descripción del riesgo"

La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en el numeral 12.5. de esta política. 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 dentro 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 a continuación:

Impacto	Causa inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e	

COPIA CONTROLADA

		independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]".	
	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

En ese orden de ideas, para cada riesgo y su causa inmediata, atendiendo la estructura para la redacción del riesgo definida en el numeral 12.5 se tendría lo siguiente:

• Posibilidad de afectación económica por Corrupción en la evaluación en la evaluación de los procesos de selección para la contratación de bienes y servicios de la Entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico.

COPIA CONTROLADA

• 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 siguiente tabla:

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

Análisis riesgos LA/FT/FP

• 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

COPIA CONTROLADA

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 los Riesgos Generales de la Gestión 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 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, debe considerarse que, además de la Política para la Gestión Integral de Riesgos y su correspondiente Mapa de Riesgos, las entidades deben elaborar, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), un Manual para la aplicación del principio de debida diligencia, disponer de una función de cumplimiento y desarrollar diversas herramientas de gestión. En conjunto, estos elementos adicionales constituyen el repertorio de controles con los que cuenta la entidad y que pueden aplicarse a cada uno de los riesgos identificados, sin perjuicio de que se incorporen controles adicionales o más específicos cuando sea necesario.

COPIA CONTROLADA

Asimismo, se recomienda que las políticas, procedimientos o códigos que se definan como controles se integren en la Política para la Gestión Integral de Riesgos o en el Programa de Transparencia y Ética Pública, con el fin de garantizar la coherencia y articulación del Sistema.

Finalmente, para el diseño y análisis de controles, debe tenerse cuenta la estructura general, los atributos y las 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 13.6. Nivel de Riesgo (Riesgo Residual) de la presente guía.

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

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.

COPIA CONTROLADA

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 expuesto, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), cada entidad deberá disponer de un Manual que integre mecanismos orientados a desarrollar el principio de debida diligencia en todas las interacciones con sus contrapartes que impliquen exposición a riesgos para la integridad pública. Esto incluye aquellas situaciones en las que se haya identificado riesgo de soborno, fraude, manejo inadecuado de conflictos de interés, corrupción, lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva.
El principio de debida diligencia se concreta a través de políticas y procedimientos destinados a identificar, analizar y evaluar los riesgos y oportunidades asociados a una interacción, operación o relación con contrapartes, con el fin de adoptar decisiones debidamente informadas. En este sentido, su aplicación debe estar alineada con los principios de razonabilidad y proporcionalidad. La razonabilidad implica que los mecanismos establecidos sean adecuados para los fines perseguidos y necesarios para su logro, mientras que la proporcionalidad supone que dichos mecanismos se apliquen con base en un enfoque de gestión del riesgo. En consecuencia, el Manual debe: (1) diseñarse de manera que su cumplimiento sea viable para la entidad, considerando los recursos disponibles (razonabilidad); y (2) prever distintos niveles de complejidad en su aplicación, de acuerdo con el nivel de riesgo que represente cada situación para la organización (proporcionalidad).

El conocimiento de las contrapartes implica la recopilación de información sobre estas, así como sobre las operaciones y los productos vinculados a la relación, con el fin de que la entidad pueda gestionar de manera adecuada los riesgos

COPIA CONTROLADA

asociados. Los resultados de estos mecanismos tienen como finalidad exclusiva servir de insumo para la toma de decisiones y no podrán dar lugar a inhabilidades o incompatibilidades distintas a las previstas en la normativa vigente. No obstante, en el marco de la gestión del riesgo, la entidad sí podrá definir y aplicar consecuencias derivadas del nivel de conocimiento alcanzado sobre sus contrapartes, entre las cuales se incluyen:

✓ 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, dado que el conocimiento de las contrapartes tiene un carácter preventivo, los mecanismos correspondientes deben aplicarse con anterioridad al establecimiento de cualquier relación. No obstante, ello no impide que se realice un monitoreo permanente y continuo durante la vigencia del relacionamiento, con el propósito de identificar cambios que puedan afectar el nivel de riesgo.
La entidad deberá asegurar que los resultados derivados de la aplicación de los mecanismos de conocimiento de las contrapartes queden debidamente documentados al interior de la organización. Para tal efecto, deberá garantizar la confidencialidad de la información clasificada y reservada, el adecuado tratamiento de los datos personales, así como su correcta conservación, archivo y custodia, de conformidad con la normativa vigente.

Todo lo anterior deberá estar debidamente incorporado en el Manual que elabore la entidad, el cual deberá cumplir con las siguientes características:

1. Establecer lineamientos de debida diligencia:

COPIA CONTROLADA

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.

COPIA CONTROLADA

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. Definir un procedimiento para la verificación de la identidad de las contrapartes y la evaluación de su historial, como elemento esencial para la detección de posibles vínculos con actividades sospechosas. Para tal efecto, se deberá:

a. Identificar el nombre o la razón social de la contraparte.

b. Verificar su existencia y representación legal. En el caso de personas naturales, mediante la cédula de ciudadanía; para personas jurídicas, a través de los certificados expedidos por las cámaras de comercio; y para otras estructuras, mediante su acto de constitución y el Registro Único Tributario, cuando aplique.

c. Tratándose de personas jurídicas u otras estructuras, identificar la estructura de propiedad y la existencia de situaciones de control.

d. En el caso de personas jurídicas u otras estructuras, identificar a los beneficiarios finales.

e. Evaluar las relaciones sostenidas por la contraparte con entidades de naturaleza similar durante los dos (2) años previos al inicio del relacionamiento, siempre que la contraparte cuente con al menos dos años de existencia. Para este fin, la

COPIA CONTROLADA

entidad podrá solicitar referencias de, como mínimo, dos entidades similares con las que haya tenido relación.

f. Determinar si la contraparte dispone de un Programa de Transparencia y Ética Pública o Empresarial, o de políticas en materia de prevención de lavado de activos, antisoborno o anticorrupción.

g. Verificar la documentación presentada para sustentar cualquier aspecto relevante de la relación, tales como formación, experiencia, capacidad financiera y organizacional, entre otros.

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, penal o judicial, que estén activos o en curso ante las autoridades colombianas.

Toda esta información tiene como finalidad garantizar que la entidad comprenda de manera clara el propósito y la naturaleza de la interacción o relación que se pretende establecer. No obstante, en aplicación del principio de proporcionalidad y bajo un enfoque basado en riesgos, no en todos los casos será necesario recabar la totalidad de la información señalada. En este sentido, cada entidad podrá definir en su Manual criterios diferenciados para la aplicación de una debida diligencia simplificada en relaciones de bajo riesgo, una debida diligencia estándar para aquellas de riesgo medio, y una debida diligencia ampliada cuando se trate de escenarios de alto riesgo.

El listado de verificación previsto en esta Guía tiene un carácter meramente enunciativo. En consecuencia, cada entidad podrá incorporar en su Manual otras verificaciones adicionales relacionadas con la identificación de las contrapartes y la evaluación de su historial, conforme a sus necesidades, capacidades y criterios institucionales.

4. Definir un lineamiento específico para los casos en los que se identifique que una contraparte ostenta la condición de Persona Expuesta Políticamente (PEP), conforme a la definición prevista en el artículo 2.1.4.2.3 del Decreto 1081 de 2015. Al respecto, es importante precisar que dicha condición se mantiene

COPIA CONTROLADA

durante el ejercicio del cargo y por un período adicional de dos (2) años contados a partir de la dejación del mismo, ya sea por renuncia, despido, declaración de insubsistencia del nombramiento, cualquier otra forma de desvinculación o la terminación del contrato. En estos escenarios, la aplicación de la debida diligencia deberá contemplar un análisis más exhaustivo, en atención a que este tipo de contrapartes puede estar expuesto a mayores riesgos para la integridad pública.

5. Definir lineamientos para la toma de decisiones con base en los resultados obtenidos de la debida diligencia:

   a. El Manual deberá identificar los procesos en los cuales deben aplicarse los mecanismos de conocimiento de las contrapartes, incluyendo aquellos en los que se hayan identificado riesgos para la integridad pública. En cada uno de estos procesos, deberán precisarse las operaciones, vinculaciones o relaciones que presenten exposición a dichos riesgos.

   b. El Manual deberá establecer, como política institucional, la incorporación de un punto de control en todos los procesos en los que se identifiquen operaciones, vinculaciones o relaciones expuestas a riesgos para la integridad pública, orientado a la aplicación de los mecanismos de conocimiento de las contrapartes.

   c. Adicionalmente, la política deberá definir la forma en que se analizarán y discutirán los hallazgos, así como el procedimiento para la adopción de decisiones respecto a la continuidad, modificación o cancelación de la operación, vinculación o relación correspondiente.

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

a) En el Manual, la entidad deberá incorporar una política que defina el margen de actuación frente a posibles hallazgos, incluyendo los ajustes que puedan realizarse a los términos del acuerdo con el fin de mitigar los riesgos identificados.

COPIA CONTROLADA

b) Es importante precisar que la debida diligencia no conduce necesariamente, en todos los casos, a la configuración de una inhabilidad; no obstante, los hallazgos que se identifiquen deberán ser analizados y gestionados de manera adecuada.

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) La política deberá establecer la obligación de la entidad de realizar un monitoreo permanente de las operaciones efectuadas por la contraparte durante toda la vigencia de la relación o vinculación, con el fin de contrastarlas con los hallazgos identificados y verificar que dichas operaciones sean coherentes con el conocimiento que se tiene de la contraparte, su actividad económica y su perfil de riesgo.

✓ No contar con una identificación completa de la contraparte, incluyendo la falta de información sobre sus beneficiarios finales.

✓ La existencia de investigaciones, procesos activos o en curso que involucren a la contraparte, así como la identificación de referencias negativas o antecedentes desfavorables en la revisión de su reputación. En el caso de personas jurídicas u otras estructuras, esta verificación se extenderá al representante legal principal y suplente, al revisor fiscal, a los miembros de la junta directiva, a los controlantes y al beneficiario final.

✓ La existencia de precios significativamente diferentes a los habituales del mercado, aun cuando no se hayan calificado como artificiales.

✓ El financiamiento de la contraparte con recursos provenientes del exterior, originados en países no cooperantes o en jurisdicciones consideradas de riesgo, conforme a lo establecido por la normativa nacional vigente.

✓ Que la naturaleza de la relación implique la participación de subcontratistas por parte de la contraparte.

COPIA CONTROLADA

✓ La inclusión de la contraparte en listados internacionales vinculantes para el país, relacionados con personas o entidades asociadas con organizaciones terroristas. En el caso de personas jurídicas u otras estructuras, esta condición será aplicable al representante legal principal y suplente, al revisor fiscal, a los miembros de la junta directiva, a los controlantes y al 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.

17.3.5.3. Función de Cumplimiento

La función de cumplimiento comprende, entre otras responsabilidades, las siguientes:

✓ Asegurar el funcionamiento efectivo, eficiente y oportuno del SIGRIP, tanto de manera integral como en cada uno de sus componentes, promoviendo la observancia de sus disposiciones y apoyando a los líderes de proceso y gestores de riesgo en la administración de los riesgos identificados. Para tal efecto, podrá proponer y emitir políticas o procedimientos internos de carácter vinculante para la organización.

✓ Realizar evaluaciones periódicas del SIGRIP y presentar sus resultados a la Alta Dirección, de conformidad con la periodicidad establecida. Dichas evaluaciones deberán incluir, como mínimo:

- Los resultados de la gestión desarrollada en el ejercicio de la función de cumplimiento.

COPIA CONTROLADA

- Los reportes de operaciones generados en el marco de la gestión del riesgo.
- El avance y efectividad de los planes de mejoramiento del SIGRIP implementados, en el contexto del proceso de mejora continúa.

✓ Analizar, revisar y recomendar la adopción de los lineamientos, directrices y disposiciones emitidas por 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, en lo relacionado con la gestión del riesgo.

✓ Impulsar la adopción de acciones correctivas para el fortalecimiento del SIGRIP y ejecutar aquellas que se encuentren dentro del ámbito de su competencia.

✓ Coordinar con las dependencias correspondientes las acciones necesarias para garantizar la operatividad del SIGRIP, así como para el diseño y ejecución de programas internos de capacitación en materia de cumplimiento y gestión del riesgo.

✓ Proponer a la Alta Dirección la actualización de los elementos que conforman el SIGRIP y velar por su divulgación oportuna a todas las partes interesadas.

✓ Participar en el diseño y aplicación de las metodologías, modelos e indicadores cualitativos y/o cuantitativos requeridos para la adecuada gestión del SIGRIP.

✓ Definir los lineamientos institucionales para la aplicación proporcional y basada en riesgos de los mecanismos de debida diligencia en el conocimiento de las contrapartes.

✓ Elaborar y someter a consideración de la Alta Dirección los criterios objetivos para la identificación y clasificación de operaciones inusuales y sospechosas.

✓ Reportar oportunamente a la Unidad de Información y Análisis Financiero, a la Fiscalía General de la Nación o a la autoridad competente, las operaciones intentadas o sospechosas identificadas, de conformidad con los criterios establecidos y el procedimiento institucional vigente.

COPIA CONTROLADA

No se requiere que las entidades públicas creen cargos específicos para el ejercicio de la función de cumplimiento. De conformidad con lo dispuesto en el Decreto 1083 de 2015, esta función podrá ser asumida, como regla general, por un servidor del nivel directivo, o su equivalente según el sistema de empleo público adoptado por la entidad, en atención a que se encuentra alineada con las funciones propias de dicho nivel, en particular, la de adelantar las gestiones necesarias para garantizar el oportuno cumplimiento de los planes, programas y proyectos, así como la adopción de sistemas o canales de información que permitan su adecuada ejecución y seguimiento.

Adicionalmente, la función de cumplimiento podrá ser asignada a servidores del nivel asesor, quienes, dentro de sus responsabilidades, cuentan con la de atender consultas, brindar asistencia técnica, emitir conceptos y aportar elementos de juicio para la toma de decisiones relacionadas con la formulación, ejecución y control de los programas propios de la entidad.

Con fundamento en las consideraciones expuestas, resulta procedente señalar que la función de cumplimiento puede ser asignada dentro de las plantas de personal existentes en la mayoría de las entidades públicas, sin perjuicio de que, en ejercicio de su autonomía administrativa, la entidad opte por la creación de un cargo específico para tal fin.

En este sentido, para la asignación de la función de cumplimiento deberán considerarse, como mínimo, los siguientes aspectos:

✓ La función podrá ser asignada a una persona, grupo o dependencia, de acuerdo con las capacidades institucionales. Para tal determinación, se recomienda evaluar la estructura organizacional, la planta de personal y las cargas de trabajo, la complejidad de las operaciones y el nivel de exposición a los riesgos para la integridad pública, a fin de definir la capacidad requerida de quien asuma la función de cumplimiento.

✓ La función deberá estar ubicada en el segundo nivel jerárquico de la entidad, de manera que la persona, grupo o dependencia responsable dependa directa y exclusivamente de la Alta Dirección.

✓ De manera preferente, la persona, grupo o dependencia designada deberá dedicarse de forma exclusiva al ejercicio de la función de cumplimiento. No obstante, cuando esta sea asignada a quien desempeñe funciones adicionales y

COPIA CONTROLADA

no cuente con dedicación exclusiva, la entidad deberá establecer mecanismos adecuados para prevenir, identificar y gestionar los posibles conflictos de interés que se deriven del ejercicio concurrente de otras funciones susceptibles de evaluación.

✓ La entidad deberá garantizar que la persona, grupo o dependencia a la cual se asigne la función de cumplimiento reciba capacitación permanente en materia de gestión de riesgos, transparencia, integridad, sistemas de gestión antisoborno, antifraude y cumplimiento, y que, adicionalmente, se mantenga actualizada respecto de los lineamientos de la Política Nacional contra el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva.

✓ La persona a quien se asigne la función de cumplimiento, así como quienes integren el grupo de trabajo o dependencia correspondiente, deberán ser reconocidos dentro de la entidad por su integridad, probidad y conducta ética, y cumplir de manera diligente con sus obligaciones. En consecuencia, no deberán registrar investigaciones de ningún tipo en su contra, deberán contar con evaluaciones de desempeño satisfactorias y haber presentado oportunamente las declaraciones de bienes y rentas y de conflictos de interés, manteniéndolas actualizadas conforme a la normativa vigente.

✓ La persona designada para ejercer la función de cumplimiento podrá asumir, adicionalmente, el rol de administrador del Programa de Transparencia y Ética Pública de la entidad.

Una vez asignada la función de cumplimiento dentro de la estructura organizacional, la entidad deberá informar a la Secretaría de Transparencia de la Presidencia de la República el nombre, número telefónico y correo electrónico de la persona designada o de quien lidere el grupo o dependencia responsable. La entidad deberá asegurar que dicha información se mantenga actualizada y, en caso de presentarse cambios, informarlos a la Secretaría dentro del mes siguiente a la ocurrencia de la novedad. Este trámite tendrá carácter exclusivamente informativo y no condiciona el ejercicio de la función, ni implica la obligación de surtir posesión o formalidad adicional ante la Secretaría de Transparencia.

La función de cumplimiento no reemplaza, limita ni menoscaba las funciones propias de las unidades de control interno de la entidad.

COPIA CONTROLADA

De manera excepcional, la entidad podrá contratar a particulares para apoyar la gestión de cumplimiento. En estos eventos, deberá adelantarse el respectivo proceso de selección de conformidad con lo dispuesto en el Estatuto General de Contratación de la Administración Pública, el cual deberá atender, como mínimo, las siguientes consideraciones:

a. La contratación solo procederá cuando la entidad acredite que no cuenta con personal suficiente en su planta para asumir la función de cumplimiento. Dada la especial relevancia de esta función, el certificado de inexistencia de personal deberá estar suscrito por el representante legal de la entidad y contener un análisis integral de la estructura organizacional y de la planta de personal, que permita concluir de manera inequívoca que la función no puede ser asignada a ningún servidor de los niveles directivo o asesor.

b. Deberán contratarse servicios profesionales especializados. Para tal efecto, la entidad deberá establecer en los documentos del proceso, como requisitos mínimos, los siguientes: (i) formación específica en materias relacionadas con cumplimiento, gestión del riesgo de LA/FT/FP o áreas conexas al SIGRIP; y (ii) experiencia específica y relacionada mínima de un (1) año en gestión del riesgo en entidades públicas, gestión del riesgo de LA/FT/FP o en el ejercicio del rol de oficial de cumplimiento.

b. En los documentos del proceso deberá incorporarse un requisito mediante el cual se establezca que, al momento de la presentación de la oferta, el oferente no podrá encontrarse vinculado a más de tres (3) entidades públicas prestando servicios de apoyo a la gestión de cumplimiento. Así mismo, deberá exigirse una declaración en la que el oferente informe si mantiene vínculos contractuales con otras entidades públicas para la prestación del mismo servicio o de servicios similares de apoyo a la gestión de cumplimiento.

17.3.5.4. 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.

COPIA CONTROLADA

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 adoptar una política institucional en la que se establezca de manera expresa el compromiso de la Alta Dirección con la promoción de una cultura orientada a la prevención y mitigación de los riesgos de lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva. Dicha política deberá prohibir y rechazar cualquier práctica asociada a estos riesgos, exigir el cumplimiento estricto de la normativa ALA/CFT/CFP vigente, establecer la obligación de aplicar mecanismos de debida diligencia en el conocimiento de las contrapartes, fomentar la denuncia de actividades relacionadas con las señales de alerta definidas por la entidad sin temor a represalias, e informar claramente las consecuencias derivadas del incumplimiento de sus disposiciones.

b. Política Antisoborno.
La entidad deberá formular una política institucional que declare de forma expresa el compromiso de la Alta Dirección con una cultura de prevención y mitigación del soborno. Esta política deberá definir y tipificar las conductas constitutivas de soborno, prohibir y rechazar cualquier práctica relacionada con este, exigir el cumplimiento de la normativa antisoborno aplicable, establecer la obligación de actuar con debida diligencia en el conocimiento de las contrapartes, promover la denuncia de actividades vinculadas con las señales de alerta establecidas por la entidad sin riesgo de represalias, e informar las consecuencias del incumplimiento de la política.

c. Política Antifraude.
La entidad deberá adoptar una política institucional que manifieste expresamente el compromiso de la Alta Dirección con una cultura de prevención y mitigación del fraude. Dicha política deberá identificar y tipificar las prácticas de fraude, prohibir y rechazar cualquier conducta asociada a este riesgo, exigir el cumplimiento de la normativa antifraude vigente, promover la denuncia de actividades relacionadas con las señales de alerta definidas por la entidad sin temor a represalias, e informar de manera clara las consecuencias del incumplimiento de la política.

d. Procedimiento para la gestión de los conflictos de interés.

COPIA CONTROLADA

La entidad deberá adoptar un procedimiento interno que contemple de manera expresa un catálogo de situaciones susceptibles de generar conflictos de interés dentro de la organización, acompañado de ejemplos ilustrativos. Dicho procedimiento deberá establecer de forma clara el paso a paso que deberán seguir los servidores, contratistas o demás partes involucradas para declarar un conflicto de interés, así como el procedimiento que seguirá la entidad para su análisis y trámite. Adicionalmente, deberá definir el margen de actuación institucional para la gestión de los conflictos de interés, el procedimiento para la presentación de las declaraciones periódicas exigidas por la ley y los mecanismos para verificar el cumplimiento oportuno de dichas declaraciones.

e. Procedimiento para el reporte de operaciones sospechosas.
La entidad deberá formular un procedimiento interno que establezca de manera expresa los criterios y señales de alerta para la identificación de operaciones inusuales. Así mismo, deberá definir el paso a paso mediante el cual los líderes de proceso reportarán dichas operaciones a quien ejerza la función de cumplimiento, el procedimiento que seguirá este último para evaluar las operaciones inusuales y determinar si tienen la calidad de sospechosas, y el proceso para efectuar el reporte correspondiente a las autoridades competentes, incluso cuando se trate de operaciones intentadas.

f. Procedimiento para la operación del canal institucional de denuncias por corrupción y buzón ético.

La entidad deberá establecer un procedimiento interno que identifique los diferentes medios habilitados para la recepción de denuncias e inquietudes, así como el paso a paso para su evaluación, tratamiento y gestión a través del canal institucional. El procedimiento deberá, además, definir las etapas para la conclusión del trámite de las denuncias e inquietudes, de conformidad con el análisis y tratamiento efectuados.

Todas las herramientas de gestión deberán ser desarrolladas e incorporadas en los Programas de Transparencia y Ética Pública de las entidades. En este sentido, la Política para la Gestión Integral de Riesgos, el Mapa de Riesgos y el Manual de Debida Diligencia en el Conocimiento de las Contrapartes hacen parte integral del Programa de Transparencia y Ética Pública.

La Secretaría de Transparencia de la Presidencia de la República pondrá a disposición de las entidades herramientas modelo que podrán ser adoptadas de

COPIA CONTROLADA

manera voluntaria. Lo anterior se entiende sin perjuicio de que, igualmente de forma voluntaria, las entidades opten por implementar sistemas estandarizados en aquellas herramientas de gestión que cuenten con guías o normas técnicas expedidas por organismos de normalización reconocidos.

17.3.6. Monitoreo, evaluación, auditoría y mejora

El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) deberá estar sujeto de manera continua a procesos de seguimiento, evaluación, auditoría y mejora permanente. Para tal efecto, se deberán considerar los siguientes aspectos:

✓ Corresponde al Administrador del Programa, en su calidad de segunda línea de defensa, realizar la evaluación de la gestión del riesgo. Esta evaluación comprende la verificación del cumplimiento de los objetivos definidos para el SIGRIP y para cada uno de sus componentes. Para tal efecto, el Administrador deberá medir y analizar los resultados del monitoreo, con el fin de efectuar una valoración objetiva, considerando los indicadores de gestión del riesgo que se establezcan y los reportes requeridos a la primera línea de defensa. En la Política para la Gestión Integral de Riesgos deberán definirse la periodicidad y el alcance de la evaluación del SIGRIP.

✓ El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) deberá ser objeto de auditoría, la cual estará a cargo de la unidad de control interno o de quien ejerza la función de tercera línea de defensa. La auditoría tendrá por objeto realizar una evaluación independiente del Sistema, a fin de determinar su conformidad y eficacia, tanto de manera integral como respecto de cada uno de sus controles. Esta labor deberá desarrollarse conforme a las técnicas de auditoría vigentes, al plan anual de auditoría de la entidad y bajo un enfoque basado en riesgos. En la Política para la Gestión Integral de Riesgos deberán establecerse los criterios de auditoría aplicables al SIGRIP.

✓ La mejora del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) será responsabilidad de la Alta Dirección, en su rol de línea estratégica, a través de la revisión integral del Sistema. Este proceso deberá ser continuo y alimentarse de la información proveniente del monitoreo, las evaluaciones y las auditorías realizadas. En todo caso, deberán implementarse los planes de mejoramiento necesarios para atender los hallazgos y no conformidades identificados, sin perjuicio de considerar, desde

COPIA CONTROLADA

un enfoque preventivo, los resultados de las evaluaciones y del monitoreo. En la Política para la Gestión Integral de Riesgos deberá definirse expresamente el proceso de mejora continua del SIGRIP.

COPIA CONTROLADA