Ambiente

Guía para la Gestión Integral del riesgo

Proceso

Administración del Sistema Integrado de Gestión

Versión 10

30/06/2026

TABLA DE CONTENIDO

1 INTRODUCCIÓN 6

2 OBJETIVO 7

3 ALCANCE 7

4 DEFINICIONES O CONCEPTOS 7

5 MARCO REGULATORIO O NORMATIVO 15

6 RESPONSABILIDAD 17

7 METODOLOGÍA PARA LA ADMINISTRACIÓN Y GESTIÓN DEL RIESGOS. 19

7.1 POLÍTICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS 20
7.1.1 DETERMINACIÓN DE LA CAPACIDAD DE RIESGO 20
7.1.2 DETERMINACIÓN DEL APETITO DE RIESGO 21
7.1.3 TOLERANCIA DE RIESGO 21

CAPÍTULO I RIESGOS GENERALES DE LA GESTIÓN 23

7.2 PASO 1 IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO 23
7.2.1 ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS 23
7.2.2 NIVELES DE MADUREZ PARA LA GESTIÓN DEL RIESGO 24
7.2.3 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO 25
7.2.4 IDENTIFICACIÓN DE ÁREAS DE IMPACTO 25
7.2.5 IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO 25
7.2.6 DESCRIPCIÓN DE RIESGOS 29
7.3 PASO 2 ANÁLISIS DE RIESGO INHERENTE 31
7.3.1 DETERMINAR LA PROBABILIDAD 31
7.3.2 DETERMINAR EL IMPACTO 32
7.3.3 ANÁLISIS DE SEVERIDAD 34
7.4 PASO 3 DISEÑO Y ANÁLISIS DE CONTROLES 35
7.4.1 VALORACIÓN DE CONTROLES 35
7.4.2 ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL 36
7.4.3 TIPOLOGÍAS DE CONTROLES 38
7.4.4 VALORACIÓN DE CONTROLES 39
7.4.5 APLICACIÓN DE CONTROLES EN LA MATRIZ DE SEVERIDAD 40
7.5 PASO 4: VALORACIÓN DE RIESGO RESIDUAL 40
7.5.1 CONSOLIDACIÓN MAPA DE RIESGOS INTEGRAL 43
7.6 SEGUIMIENTO, MONITOREO Y REVISIÓN EN EL MARCO DEL ESQUEMA DE LÍNEAS DEL MODELO ESTÁNDAR DE CONTROL INTERNO MECI 43
7.6.1 INDICADORES PARA EL SEGUIMIENTO 43
7.6.2 ALCANCE DE LOS INDICADORES CLAVE DE PROCESO (KPI) Y LOS INDICADORES CLAVE DE RIESGO (KRI) 44
7.6.3 MONITOREO Y REVISIÓN 46

7.6.4 RIESGOS MATERIALIZADOS ... 51

8 COMUNICACIÓN Y CONSULTA ... 52

CAPITULO II. GESTIÓN PREVENTIVA DE RIESGOS FISCALES ... 53

9 ARTICULACIÓN MODELO CONSTITUCIONAL CONTROL FISCAL Y SISTEMA DE CONTROL INTERNO ... 53

9.1 PASO 1 IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO ... 54
9.1.1 PASOS PARA LA IDENTIFICACIÓN DEL RIESGO FISCAL ... 54
9.1.2 PUNTOS DE RIESGO Y LAS CIRCUNSTANCIAS INMEDIATAS ... 54
9.1.3 IDENTIFICAR EL ÁREA DE IMPACTO ... 59
9.1.4 IDENTIFICAR EL EFECTO ECONOMICO ... 59
9.1.5 IDENTIFICAR LA CAUSA RAIZ O POTENCIAL HECHO GENERADOR ... 60
9.2 PASO 2: ANÁLISIS RIESGO INHERENTE ... 62
9.3 PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES ... 62
9.4 PASO 4: VALORACIÓN DE RIESGO RESIDUAL ... 62

CAPÍTULO III SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA -SIGRIP ... 63

10 SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA ... 63

10.1 AMENAZAS PARA LA INTEGRIDAD PÚBLICA ... 63
10.2 CONTEXTO DE LA ORGANIZACIÓN ... 65
10.3 OPERATIVIDAD DE LOS RIESGOS PARA LA INTEGRIDAD PÚBLICA ... 65
10.4 PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO ... 65
10.4.1 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO LA/FT/FP ... 65
10.4.2 IDENTIFICACIÓN DE ÁREAS DE IMPACTO LA/FT/FP ... 66
10.4.3 IDENTIFICACIÓN DE FACTORES DE RIESGO ... 66
10.4.4 DESCRIPCIÓN DEL RIESGO ... 67
10.5 PASO 2: ANÁLISIS DE RIESGO INHERENTE ... 69
10.6 PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES ... 69
10.7 PASO 4: VALORACIÓN DE RIESGO RESIDUAL ... 69

CAPÍTULO IV RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ... 70

10.8 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN ... 70
10.9 PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN ... 71
10.9.1 TIPO DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN ... 73
10.9.2 TIPO DE RIESGOS FRENTE A LOS DATOS PERSONALES ... 74
10.9.3 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES ... 74
10.9.4 IDENTIFICACIÓN DE CONSECUENCIAS ... 80
10.10 PASO 2: ANÁLISIS DE RIESGO INHERENTE ... 81
10.11 PASO 3: IDENTIFICACIÓN DE CONTROLES ... 81
10.11.1 DOMINIO ... 82
10.11.2 CONTROLES ISO 27001 ... 82
10.12 PASO 4: VALORACIÓN DE RIESGO RESIDUAL ... 85
10.13 REVISIÓN Y MONITOREO ... 85

CAPÍTULO V RIESGOS AMBIENTALES ... 86

10.14 PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO AMBIENTAL 86
10.15 PASO 2. ANÁLISIS DE RIESGO INHERENTE RIESGO AMBIENTAL 87
10.16 PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES RIESGOS DEL SGA. 87
10.17 PASO 4: VALORACIÓN DEL RIESGO RESIDUAL. 87

CAPÍTULO VI RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO 88

LISTA DE TABLAS

Tabla 1. *Características SMART.* 23
Tabla 2. *Componentes y principios evaluables modelo de madurez* 24
Tabla 3. *Factores para cada categoría del contexto* 26
Tabla 4. *Factores de riesgo* 28
Tabla 5. *Premisas redacción del riesgo* 30
Tabla 6. *Frecuencia de actividades relacionadas con la gestión* 31
Tabla 7. *Criterios para definir el nivel de probabilidad* 32
Tabla 8. *Criterios para definir el nivel de impacto* 32
Tabla 9. *Valoración del control* 39
Tabla 10. *Análisis atributos para la formalización del control* 39
Tabla 11. *Alcance aplicación KPI y KRI* 44
Tabla 12. *Ejemplos indicadores clave de riesgo* 45
Tabla 13. *Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas* 55
Tabla 14. *Preguntas orientadoras identificación riesgo fiscal* 58
Tabla 15. *Ejemplos acorde con el objeto sobre el que recae el efecto dañoso* 61
Tabla 16. *Amenazas para la Integridad Pública* 64
Tabla 17. *Ejemplos descripción del riesgo LA/FT/FP* 67
Tabla 18. *Análisis riesgos LA/FT/FP* 68
Tabla 19. *Clasificación de los activos de información* 72
Tabla 20. *Clasificación tipos de riesgo digital* 73
Tabla 21. *Tipos de riesgo de bases de datos personales* 74
Tabla 22. *Amenazas comunes* 75
Tabla 23. *Vulnerabilidades comunes* 77
Tabla 24. *Consecuencias riesgos seguridad de la información* 80
Tabla 25. *Ejemplo identificación de controles seguridad de la información* 82
Tabla 26. *Lista de dominios anexo A* 82
Tabla 27. *Controles Anexo A ISO27001:2022* 82

LISTA DE IMÁGENES

Imagen 1. *Estructura Guía para la Gestión Integral del Riesgo* 6
Imagen 2. *Metodología para la Administración del Riesgo.* 19
Imagen 3. *Apetito, tolerancia y capacidad de riesgo* 22
Imagen 4. *Estructura propuesta para la redacción del riesgo* 29
Imagen 5. *Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo* 31
Imagen 6. *Ejemplo aplicado a tablas de probabilidad e impacto.* 33
Imagen 7. *Matriz de calor (niveles de severidad del riesgo)* 34
Imagen 8. *Ejemplo aplicado matriz de calor* 35
Imagen 9. *Estructura para la redacción de controles* 37
Imagen 10. *Ejemplo aplicado redacción del control.* 37
Imagen 11. *Cadena de valor del proceso y tipologías de controles.* 38
Imagen 12. *Movimiento en la matriz de calor acorde con el tipo de control.* 40
Imagen 13. *Ejemplo aplicado a la tabla de análisis atributos para la formalización del control* 41
Imagen 14. *Movimiento en la matriz de calor con el ejemplo propuesto* 41
Imagen 15. *Articulación Indicadores Clave de Riesgo y los Indicadores Clave de Proceso* 44
Imagen 16. *Articulación del Control Fiscal y Sistema de Control Interno* 53
Imagen 17. *Pasos para la identificación del riesgo fiscal* 54
Imagen 18. *Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo fiscal* 61
Imagen 19. *Estructura Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP* 63
Imagen 20. *Pasos levantamiento activos de información* 71

1 INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible, como entidad del orden público y coherente con la Política para la Gestión Integral del Riesgo, reconoce la necesidad de gestionar de manera integral los riesgos a que se encuentra expuesto y así promover el cumplimiento de su misión, objetivos estratégicos y procesos.

La presente *"Guía para la Gestión Integral del Riesgo"*, establece las orientaciones y metodología para operativizar la Política para la Gestión Integral del Riesgo aprobada por el Ministerio de Ambiente y Desarrollo Sostenible en el Comité Institucional de Coordinación de Control Interno en sesión del mes de mayo de 2026.

Además, cumple con lo señalado por el Departamento Administrativo de la Función Pública – DAFP en la *"Guía para la Gestión Integral del Riesgo en Entidades Públicas"* (versión 7 de 2025), en el Modelo Integrado de Planeación y Gestión (MIPG) y en la normatividad aplicable expedida por los entes competentes.

Esta Guía en el contexto de la gestión integral del riesgo, está estructurada por una primera parte en la cual se referencia el objetivo, alcance, definiciones, marco normativo, responsabilidades, esquema metodológico y conceptos. Una segunda parte, que señala la metodología para los riesgos de gestión, la cual será el estándar para cualquier tipo de riesgos y los capítulos siguientes contiene aspectos específicos a ser considerados sobre los Riesgos Fiscales, Sistema de Gestión de Riesgos para la Integridad Pública, Riesgos de Seguridad de la Información, Riesgos Ambientales y Riesgos de Seguridad y Salud en el Trabajo.

Imagen 1. *Estructura Guía para la Gestión Integral del Riesgo*

2 OBJETIVO

Establecer las orientaciones metodológicas para llevar a cabo la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos en el Ministerio de Ambiente y Desarrollo Sostenible, de manera que permita una gestión integral con un enfoque estratégico y preventivo

3 ALCANCE

La gestión del riesgo aplica para todos los procesos del Sistema Integrado de Gestión (estratégicos, misionales, de apoyo y de evaluación independiente) del Ministerio de Ambiente y Desarrollo Sostenible. Inicia con la identificación de los riesgos y termina con su monitoreo y seguimiento, con el fin de evidenciar el cumplimiento de las acciones planteadas.

4 DEFINICIONES O CONCEPTOS

- **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.

- **AMENAZA:** Situación potencial de un incidente de seguridad de la información, que puede causar daños a un sistema o perjudicar a una organización información (ISO 27005:2022).

- **ANÁLISIS DEL RIESGO**: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo.

- **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.

- **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.

- **CAUSAS:** 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 inmediata, pero se asocia a la misma causa inmediata.

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

  Nota: También denominada causa eficiente o causa adecuada: Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño

- **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.

- **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.

- **CONFIDENCIALIDAD:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **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)

- **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.

  Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos

- **CONTEXTO ESTRATÉGICO**: conjunto de circunstancias internas y externas que puedan generar eventos que originen oportunidades o afecten el cumplimiento de su función, misión y objetivos institucionales.
- **CONTRAPARTE**: cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización.

- **CONTROL:** Medida que permite reducir o mitigar un riesgo.

- **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 9 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)

- **CRITERIOS DE RIESGOS:** Términos de referencia sobre los cuales se evalúa la importancia de un riesgo. Estos criterios se definen con base en los objetivos de la organización y en el contexto interno y externo.

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

- **DEBIDA DILIGENCIA EN EL CONOCIMIENTO DE LA CONTRAPARTE:** 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.

- **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.

- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable a demanda por una entidad.

- **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

- **EVALUACIÓN DEL RIESGO**: Proceso de la comparación de los resultados del análisis con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **FACTORES DE RIESGO:** Son las fuentes generadoras de riesgos.

- **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

- **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.

- **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. (ISO 37001:2025)

- **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.

- **GESTOR FISCAL:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique). 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.

- **GESTIÓN INTEGRAL DE RIESGOS:** La cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo, de cara la creación, preservación y materialización de valor; implica que la gestión del riesgo se consolida a través de: i) el reconocimiento de la cultura; ii) el desarrollo de capacidades; iii) el uso de las técnicas aplicadas; iv) la integración de la estrategia y el desempeño; v) la alineación con la estrategia y objetivos clave y vi) la relación con el valor.

- **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.

- **IDENTIFICACIÓN DEL RIESGO**: Proceso que posibilita conocer los eventos potenciales, 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.

- **INFRAESTRUCTURA CRÍTICA CIBERNÉTICA:** Se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las instituciones.

- **IMPACTO:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Un único evento de seguridad de la información o una serie de ellos, no deseados o inesperados, que tienen una probabilidad matemática significativa de comprometer las operaciones de la empresa y de amenazar la seguridad de la información (ISO 27005:2022).

- **INCIDENTE:** Evento o serie de eventos de seguridad digital no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

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

- **INTEGRIDAD:** Propiedad de la información relativa a su exactitud y completitud.

- **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: 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.

- **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.

- **MAPA DE RIESGOS:** Documento con la información resultante de la gestión del riesgo.

- **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.

- **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

- **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

- **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.

- **POLÍTICAS DE ADMINISTRACIÓN DE RIESGOS**: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

- **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.

- **PROCESO:** Sistema de actividades que utilizan recursos para transformar entradas en salidas.

- **PROPIETARIO DEL RIESGO:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

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

  Nota: 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 Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.

- **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.

- **RECURSO PÚBLICO:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

- **RIESGO:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- **RIESGO AMBIENTAL:** Posibilidad de que por forma natural o por acción humana se produzca impacto en el medio ambiente.

- **RIESGO AMBIENTAL INSTITUCIONAL:** Combinación de la probabilidad de ocurrencia de un evento y de sus consecuencias sobre el desempeño ambiental de la entidad, considerando los aspectos ambientales significativos, las obligaciones de cumplimiento ambiental y los factores de contexto (incluidos cambio climático, economía circular y biodiversidad)

- **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 DE GESTIÓN**: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos.

- **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 FISCAL:** Efecto dañoso sobre recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial (acción u omisión)

- **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

- **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.

- **RIESGO RESIDUAL:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

- **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

- **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 ISO 37001:2025)

- **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.

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

- **TOLERANCIA AL 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.

- **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.

- **VALOR DEL ACTIVO**: Está determinado por el valor de la confidencialidad, integridad y disponibilidad del activo de información.

- **VALORACIÓN DEL RIESGO**: Proceso global de identificación, análisis y evaluación del riesgo.

- **VULNERABILIDAD:** Debilidad de un activo o control que puede aprovecharse para que ocurra un evento con consecuencias negativas información (ISO 27005:2022).

5 MARCO REGULATORIO O NORMATIVO

- Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
- Ley 412 de 1997 Convención Interamericana contra la Corrupción

- Ley 599 de 2000. Por la cual se expide el Código Penal.

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

- Ley 970 de 2005 Por medio de la cual se aprueba la "Convención de las Naciones Unidas contra la Corrupción", adoptada por la Asamblea General de las Naciones Unidas

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

- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

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

- Ley 1778 de 2016 Por la cual se dictan normas sobre la responsabilidad de las personas jurídicas por actos de corrupción transnacional y se dictan otras disposiciones en materia de lucha contra la corrupción

- Ley 2013 de 2019 Por medio del cual se busca garantizar el cumplimiento de los principios de transparencia y publicidad mediante la publicación de las declaraciones de bienes, renta y el registro de los conflictos de interés

- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.

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

- Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.

- Decreto 1072 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo

- Decreto 1074 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo

- Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.

- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 648 de 2017. Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.

- Decreto 338 de 2022 Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones

- Decreto 1122 de 2024. Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública.

- Decreto 1600 de 2024. Por el cual se modifica el Capítulo 1 y 3 del Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, Decreto Reglamentario Único del Sector Presidencia de la República, en lo relacionado con las Subcomisiones Técnicas de la Comisión Nacional de Moralización y la Estrategia Nacional de Lucha Contra la Corrupción.

- Resolución 02277 de 2025. Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

- Directiva Presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.

- Directiva Presidencial No. 01 de 2015. Reporte a la Secretaría de Transparencia de la Presidencia de la República de Posibles actos de corrupción o irregularidades.

- CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital

- NTC ISO 9001:2015. Sistemas de Gestión de la Calidad. Requisitos

- NTC ISO 14001:2015. Sistemas de Gestión Ambiental. Requisitos
- NTC ISO 14001:2026 Sistemas de Gestión Ambiental. Requisitos
- NTC ISO 31000 Gestión del riesgo – Directrices
- ISO 37001:2025. Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.
- NTC ISO 27000 Tecnología de la información. técnicas de seguridad. sistemas de gestión de seguridad de la información (SGSI). visión general y vocabulario.
- NTC-ISO-IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.
- NTC ISO 27005:2022 Gestión de riesgos de seguridad de la información
- Guías del Modelo de Seguridad y Privacidad de la Información (MSPI) de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
- Manual operativo Modelo Integrado de Planeación y Gestión - MIPG, - Departamento Administrativo de la Función Pública - DAFP 2024
- Guía para la Gestión Integral del Riesgo en Entidades Públicas - Departamento Administrativo de la Función Pública - DAFP 2025

6 RESPONSABILIDAD

Esta guía establece las orientaciones para la formulación del mapa de riesgos institucional siguiendo los lineamientos del Departamento Administrativo de la Función Pública -DAFP, mediante el diligenciamiento del formato F-E-SIG-28 Mapa de riesgos institucional y su consolidación mediante el documento soporte DS-E-SIG-25 Mapa de riesgos institucional.

Todos los líderes de los procesos definidos en el Sistema Integrado de Gestión del Ministerio, con su equipo de trabajo, serán responsables de la aplicación de esta metodología, la implementación de los controles definidos y su seguimiento. La responsabilidad en la implementación de los controles y acciones asociadas a la gestión del riesgo estará definida a partir de roles y no definir nombres específicos de los colaboradores.

Así mismo, la Oficina de Control Interno verificará el cumplimiento e implementación de esta guía en los procesos definidos por la entidad y la medición de la eficacia de las acciones y controles que permitan contrarrestar la materialización de los riesgos identificados. Para la actualización del mapa de riesgos

institucional se tendrán en cuenta dichas observaciones y analizar los resultados de las evaluaciones llevadas a cabo por los organismos de control.

Para el establecimiento e implementación de un Sistema de Administración de Riesgos es necesario contar con el compromiso y la definición de responsabilidades desde el Despacho del Ministerio y Viceministerios hacia todos los niveles de la entidad, por lo que se presentarán en el Comité Institucional de Gestión y Desempeño, los resultados de los seguimientos y monitoreos realizados al mapa de riesgos. Para esto, la alta dirección debe designar al representante de la alta dirección para apoyar a los líderes de procesos y demás servidores quienes son en última instancia los encargados de identificar y elaborar el mapa de riesgos.

Cuando se requiera la actualización de la presente Guía, se liderará el proceso por parte de la Oficina Asesora de Planeación con la asesoría de la Oficina de Control Interno y la participación de dependencias líderes, de acuerdo con los tipos de riesgo definidos, como se describe a continuación:

- Los riesgos de gestión, fiscales de integridad pública y de corrupción serán liderados por la Oficina Asesora de Planeación
- Los riesgos de seguridad de la información por la Oficina de Tecnologías de la Información y la Comunicación- OTIC
- Los riesgos ambientales por las dependencias líderes del Sistema de Gestión Ambiental, como lo son, Subdirección Administrativa y Financiera (Grupo de Servicios Administrativos) en conjunto con la Oficina Asesora de Planeación (Grupo de Gestión y Desempeño Institucional)
- Los riesgos específicos de Seguridad y Salud en el Trabajo serán liderados por el Grupo de Talento Humano.

Así mismo, de acuerdo con la necesidad de incluir nuevos riesgos se convocarán a las dependencias involucradas de acuerdo con sus competencias.

La gestión integral del riesgo constituye un insumo fundamental para la planeación institucional, en la medida en que proporciona información relevante para la toma de decisiones estratégicas, la definición de prioridades, la asignación de recursos y el establecimiento de acciones orientadas al cumplimiento de los objetivos institucionales. En este sentido, los resultados derivados de la identificación, análisis, valoración, tratamiento y monitoreo de los riesgos serán considerados en los procesos de planeación, seguimiento y evaluación de la gestión, así como, en las decisiones que adopte el Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación y Control Interno, con el propósito de fortalecer el desempeño institucional, la prevención de eventos que puedan afectar el logro de los objetivos y la mejora continua de la entidad.

7 METODOLOGÍA PARA LA ADMINISTRACIÓN Y GESTIÓN DEL RIESGOS.

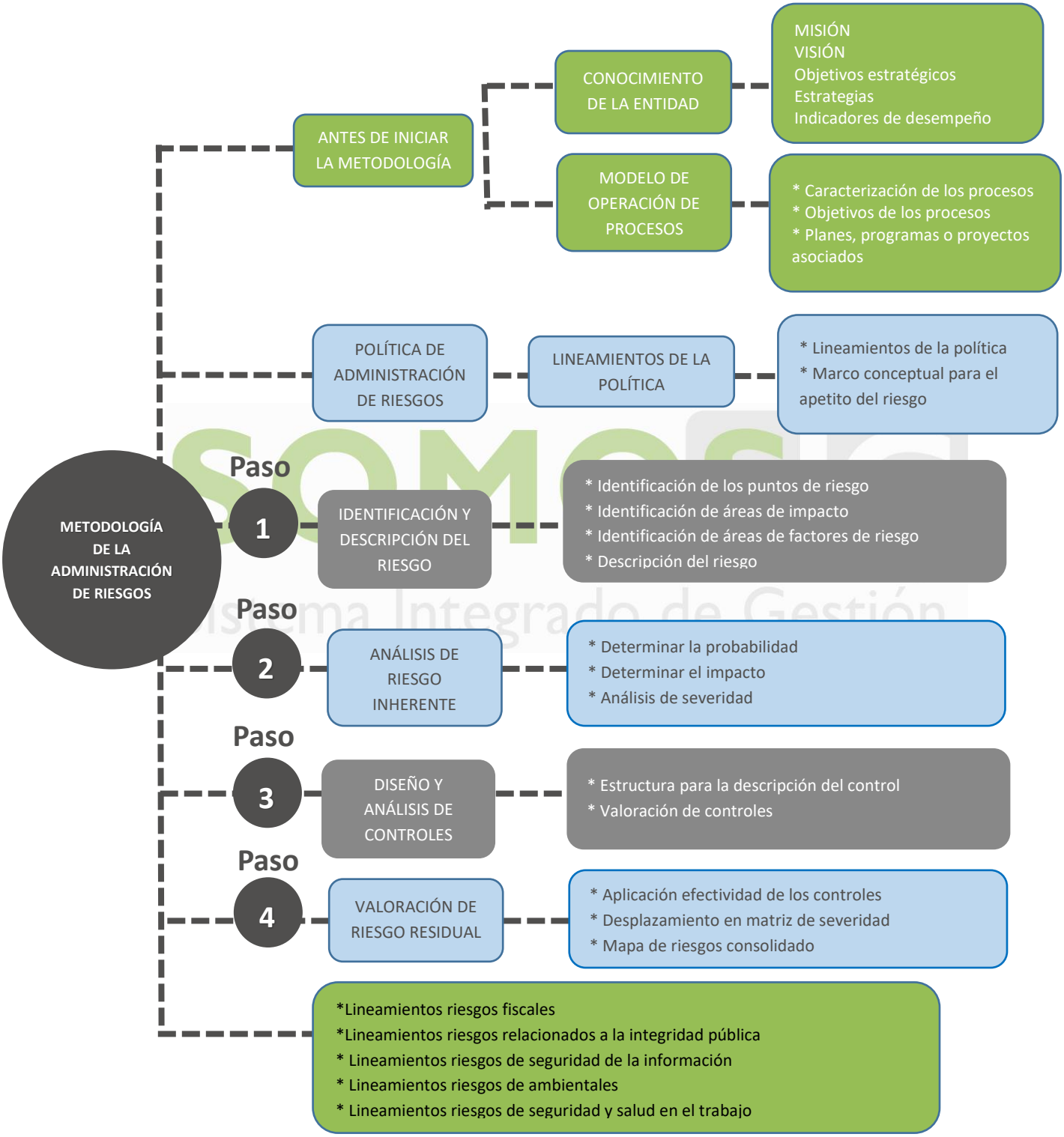

Imagen 2. *Metodología para la Administración del Riesgo.*

7.1 POLÍTICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

La Alta Dirección del Ministerio de Ambiente y Desarrollo Sostenible en conocimiento de la responsabilidad e importancia del manejo de los riesgos asociados a los diferentes procesos del Sistema Integrado de Gestión, ha documentado la Política para la Gestión Integral del Riesgo (POL-E-SIG-01) que puede ser consultada en el enlace:
https://somosig.minambiente.gov.co/portal/document_tab.php?id_doc=1555&version=1&opcion_regreso=1

Así como, las Políticas de Integridad y Lucha Contra la Corrupción (POL-E-SIG-02), orientadas a fortalecer la transparencia, la ética pública y la gestión de los riesgos de integridad. Estas incluyen:

- Políticas Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP)
- Política Antifraude
- Política Antisoborno
- Política de regalos, hospitalidad, donaciones y beneficios similares

Se pueden consultar en el siguiente enlace:
https://somosig.minambiente.gov.co/portal/document_tab.php?id_doc=1556&version=1&opcion_regreso=1

Dichas políticas fueron aprobadas en el Comité Institucional de Coordinación de Control Interno sesionado el 21 de mayo de 2026, las cuales son publicadas y comunicadas a todos los funcionarios y colaboradores del Ministerio de Ambiente y Desarrollo Sostenible a través de los diferentes medios o canales con que cuenta la entidad.

Adicionalmente, mediante la implementación de la presente Guía, se establecen las orientaciones metodológicas por medio de la cual se valoran y se hace tratamiento a los riesgos por procesos como herramienta estratégica y de gestión que permita anticipar y responder de manera oportuna y óptima a la materialización de los riesgos identificados en la matriz, contribuyendo al cumplimiento de los objetivos misionales y la mejora continua del sistema.

7.1.1 DETERMINACIÓN DE LA CAPACIDAD DE RIESGO

El Ministerio de Ambiente y Desarrollo Sostenible con la participación y aprobación de la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno debe realizar el análisis de eventos y riesgos críticos que tienen un nivel de severidad muy alto frente a los cuales se deben tomar decisiones debido a que el riesgo excede los niveles de riesgo tolerables, teniendo en cuenta los siguientes valores:

- Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
- Valor máximo del nivel de riesgo que la 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 que corresponde a la “capacidad de riesgo”.

- Corresponde al nivel más crítico de exposición al riesgo en zona de severidad extrema después de la valoración del riesgo residual; por lo tanto, requiere la implementación de controles y acciones de tratamiento orientadas a reducir su probabilidad de ocurrencia o impacto. Su gestión debe incluir un seguimiento cuatrimestral o una vez finalizada la ejecución de los controles y acciones establecidas, con el fin de verificar su efectividad y garantizar la disminución del nivel de riesgo.

7.1.2 DETERMINACIÓN DEL APETITO DE RIESGO

El "apetito de riesgo", se define como el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección en condiciones normales de operación del Modelo Integrado de Planeación y Gestión.

El Ministerio de Ambiente y Desarrollo Sostenible establece que dentro del límite de apetito de riesgo se encuentran aquellos riesgos que, una vez implementados los controles correspondientes, se clasifican en una zona de severidad baja. Para los cuales se continúa el monitoreo, con el fin de garantizar que las condiciones bajo las cuales han sido analizados no han cambiado, si las condiciones cambian, es necesario volver a valorar y si es el caso determinar el manejo correspondiente a través de los controles que sean necesarios.

Los riesgos vinculados al Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), entre los que se encuentran los riesgos de corrupción, soborno, fraude, la gestión inadecuada de conflictos de interés, la corrupción y los riesgos asociados al Lavado de Activos (LA), la Financiación del Terrorismo (FT) y la Financiación de la Proliferación de Armas de Destrucción Masiva (FP), son considerados inaceptables por la Entidad, lo cual significa que se documentarán controles y acciones de tratamiento según corresponda.

7.1.3 TOLERANCIA DE RIESGO

El límite o valor de 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. Se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad, el cual es definido por la alta dirección.

El Ministerio de Ambiente y Desarrollo Sostenible determina que forman parte de su límite de tolerancia al riesgo aquellos riesgos residuales que, tras la aplicación de los controles correspondientes, se clasifican en las zonas de severidad moderada y alta, frente a los cuales se establecen controles y acciones de plan de manejo que permitan reducir su probabilidad de ocurrencia o impacto.

Su gestión del riesgo incluye el seguimiento semestral de los controles y de las acciones implementadas, con el fin de mitigar los riesgos identificados, disminuir su nivel de exposición mediante una gestión preventiva y efectiva.

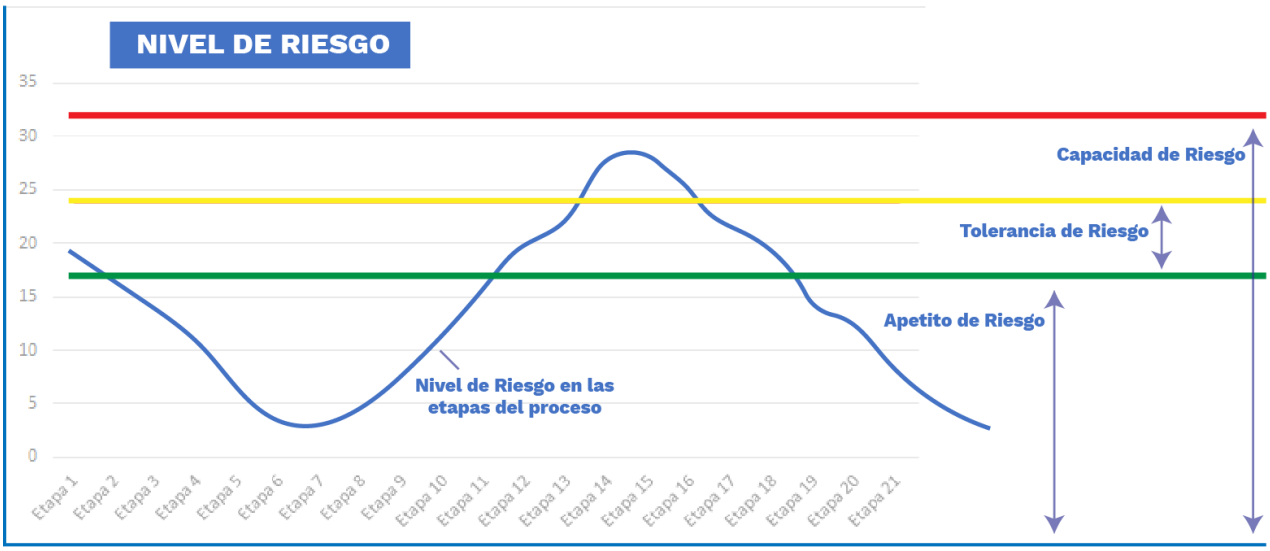

Imagen 3. *Apetito, tolerancia y capacidad de riesgo*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020. Tomado de la guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013

SOMOSIG Sistema Integrado de Gestión

CAPÍTULO I RIESGOS GENERALES DE LA GESTIÓN

A continuación, se definen los pasos para identificar y gestionar los riesgos relacionados con los riesgos estratégicos, es decir, que afecten el cumplimiento de los objetivos institucionales o del proceso.

7.2 PASO 1 IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

7.2.1 ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS

Los riesgos identificados deben tener impacto en el cumplimiento de objetivos estratégicos, estar alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos.

Para su adecuada formulación, deben contener unos atributos mínimos, para lo cual se puede hacer uso de las características SMART:

Tabla 1. *Características SMART.*

S	Específico	Resuelve cuestiones como qué, cuándo, cómo, dónde, con qué, quién considerando el orden y los necesarios para el cumplimiento de la misión.
M	Medible	Involucra algunos números en su definición. Ejemplo: porcentajes o cantidades (cuando aplique)
A	Alcanzable	Realizar un análisis de los que se ha hecho y logrado hasta el momento para determinar si lo que se propone es posible o cómo resultaría mejor
R	Realista	Considera recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación
T	Temporal	Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y las mediciones finales.

Adaptada fuente: DAFP. 2025.

De acuerdo con lo anterior, se debe tener en cuenta que los indicadores del Sistema Integrado de Gestión- SIG, permiten medir el cumplimiento del objetivo de cada proceso, alineados con la plataforma estratégica del SIG (Objetivos, política, misión y visión) y de la misma manera los riesgos se identifican a partir de los factores de riesgo que puedan afectar el cumplimiento del objetivo de cada proceso.

7.2.2 NIVELES DE MADUREZ PARA LA GESTIÓN DEL RIESGO

Con base en el nivel de madurez de la gestión del riesgo en la entidad, se podrán determinar las actividades que se espera desarrollar dentro del rol de evaluación de dicha gestión, con el propósito de que este rol aporte un mayor valor a la toma de decisiones por parte de la alta dirección, incluyendo:

Tabla 2. *Componentes y principios evaluables modelo de madurez*

1. Gobierno y cultura
Constituye la base para los demás componentes de la gestión del riesgo. El gobierno define el tono de la entidad, refuerza la importancia de la gestión del riesgo y establece las responsabilidades de supervisión. La cultura se refleja en la toma las decisiones
1. Supervisión de riesgos a través del Comité Institucional de Coordinación de Control Interno
2. Establece estructuras operativas
3. Define la cultura deseada
4. Demuestra compromiso con los valores del servicio público
5. Atrae, desarrolla, y retiene a profesionales capacitados
2. Estrategia y definición de objetivos
La gestión del riesgo se integra en el plan estratégico de la entidad a través del proceso de establecimiento de la estrategia y de los objetivos. El conocimiento del contexto permite a la Entidad comprender mejor los factores internos y externos y sus efectos en el riesgo.
6. Analiza el contexto Sectorial/Territorial e Institucional
7. Define el apetito al riesgo
8. Evalúa estrategias alternativas
9. Formula objetivos estratégicos y operacionales
3. Desempeño
Se identifican y evalúan los riesgos que pueden afectar la capacidad de la entidad para alcanzar la estrategia y los objetivos, se determinan las respuestas frente a dichos riesgos y se efectúa seguimiento del desempeño teniendo en cuenta posibles cambios.
9. Identifica y describe el riesgo
10. Evalúa el riesgo inherente
11. Diseña controles efectivos
12. Prioriza riesgos
13. Desarrolla una visión integral
4. Análisis y monitorización
Se realiza un análisis de las capacidades y técnicas de gestión del riesgo, junto con una evaluación del desempeño de la entidad frente al cumplimiento de sus objetivos
14. Evalúa los cambios significativos
15. Revisa el riesgo y el desempeño
16. Persigue la mejora de la gestión del riesgo

5. Información, comunicación y reporte
La comunicación permite compartir información relevante en toda la entidad. A través del uso de fuentes internas y externas y mediante el aprovechamiento de los sistemas de información, se facilita la gestión del riesgo e informa sobre el riesgo, la cultura y el desempeño.
17. Aprovecha la información y la tecnología
18. Comunica información sobre riesgos
19. Informa sobre el riesgo, la cultura y el desempeño

Adaptada fuente: DAFP. 2025.

7.2.3 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO

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.

Para identificar estos puntos de riesgo es importante tener en cuenta la documentación del proceso: caracterización, contexto estratégico, procedimientos, guías, protocolos, manuales, instructivos, documentos soporte y formatos, entre otros. Así como, la cadena de valor público, desde insumos, procesos, productos, resultados, efectos e impactos y el cumplimiento de los objetivos (eficacia y eficiencia).

Para la identificación del riesgo fiscal, los puntos de riesgo, pueden incluir actividades de gestión fiscal (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), así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal.

7.2.4 IDENTIFICACIÓN DE ÁREAS DE IMPACTO

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la Entidad en caso de materializarse un riesgo.

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público sobre: recursos públicos, bienes públicos o intereses patrimoniales de naturaleza pública.

7.2.5 IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Son las fuentes generadoras de riesgos, estas circunstancias o condiciones **aumentan la probabilidad de que ocurra el evento de riesgo**, pueden originarse en fuentes internas o externas, las cuales no constituyen causas directas del riesgo, pero aumentan el nivel de exposición al mismo.

La definición de los parámetros internos y externos que deben considerarse para la administración del riesgo se realiza a través del análisis de los contextos estratégicos en cada proceso. De igual manera, se identifican

todas las actividades internas y del entorno que puedan generar eventos que representen oportunidades o que puedan afectar negativamente el cumplimiento de la misión institucional y sus objetivos.

Tabla 3. *Factores para cada categoría del contexto*

CONTEXTO EXTERNO: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad	**ECONÓMICOS:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia
	MEDIOAMBIENTALES: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible, cambio climático, disponibilidad de recursos naturales, biodiversidad o salud de los ecosistemas, niveles de contaminación, economía circular, mercados verdes.
	POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación, normatividad externa (leyes, decretos, ordenanzas y acuerdos).
	SOCIALES: Demografía, responsabilidad social, orden público, área de influencia
	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea, requisitos de partes interesadas en seguridad de la información
	COMUNICACIÓN EXTERNA: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad. Sector en el que opera la entidad y su relacionamiento interinstitucional, así como, el entorno de desarrollo territorial.
CONTEXTO INTERNO: Se determinan las características o aspectos esenciales del ambiente en cual la organización busca alcanzar sus objetivos.	**FINANCIEROS:** Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada
	PERSONAL: Competencia del personal, disponibilidad del personal, seguridad y salud en el trabajo
	PROCESOS: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento, articulación de los sistemas de gestión (Sistema de Gestión de Calidad, Sistema de Gestión Ambiental, Sistema de Seguridad y Salud en el Trabajo, Sistema de Gestión de Seguridad de la Información, entre otros).
	TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano y requisitos de partes interesadas internas en seguridad de la información
	ESTRATÉGICOS: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo, valores y cultura ambiental, rendición de cuentas, responsabilidad ambiental en la cadena de mando.
	COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de todos los procesos de la entidad
	GESTIÓN AMBIENTAL: Apropiación e implementación de buenas prácticas ambientales, compras sostenibles y requisitos de economía circular, eficiencia energética, cero papel, uso de recursos naturales, toma de conciencia.

CONTEXTO DEL PROCESO: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.	**DISEÑO DEL PROCESO:** Claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a insumos, proveedores – cadena de valor, productos, usuarios o clientes, economía circular, mercados verdes.
	TRANSVERSALIDAD: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABILIDAD DEL PROCESO: Grado de autoridad y responsabilidad de los colaboradores frente al proceso.
	COMUNICACIÒN ENTRE LOS PROCESOS: Efectividad en los flujos de información determinados en la interacción de los procesos.
PARTES INTERESADAS Se determinan los requisitos frente a sus necesidades y expectativas	**CARACTERIZACIÓN DE LAS PARTES INTERESADAS:** Identificación de las partes interesadas internas y externas y los requisitos legales y otros aplicables a sus necesidades y expectativas

Adaptada fuente: DAFP. 2018

El seguimiento y la revisión del contexto estratégico se realizan anualmente en el marco de la actualización del mapa de riesgos institucional, con el propósito de identificar y analizar las condiciones o causas que pueden dar origen a los riesgos. En este ejercicio, las áreas de factores de riesgo constituyen un insumo para la identificación y evaluación de los elementos del contexto que podrían afectar el logro de los objetivos estratégicos de la entidad.

De igual manera, las oportunidades de mejora identificadas durante este proceso se documentan y gestionan mediante la formulación de acciones en el Plan de Mejoramiento Institucional, con el fin de fortalecer el desempeño institucional y promover la mejora continua.

En concordancia con el enfoque de gestión basado en riesgos, se invita a los líderes de proceso a evolucionar de un esquema de control centrado en el cumplimiento normativo hacia un modelo preventivo, mediante la racionalización y fortalecimiento del diseño de los controles. Para ello, se prioriza la implementación de controles que actúen directamente sobre la causa raíz de los riesgos, favoreciendo su tratamiento efectivo y reduciendo la probabilidad de materialización de eventos que puedan afectar el cumplimiento de los objetivos institucionales.

En la siguiente tabla se presenta el listado de factores de riesgo que pueden incidir en su generación:

Tabla 4. *Factores de riesgo*

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

Adaptada fuente: DAFP. 2025

Nota: Se debe evaluar la información proveniente de la gestión y mesa de asistencia - GEMA frente a los incidentes y casos registrados en los módulos: administrativo, apoyo a nivel tecnológico y de comunicaciones. Así mismo, evaluar información proveniente de quejas y denuncias de los usuarios y la necesidad de evaluar información proveniente de quejas y denuncias de los servidores de la entidad para la identificación de riesgos de fraude y corrupción.

7.2.6 DESCRIPCIÓN DE RIESGOS

La descripción del riesgo se realiza a partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados.

Para la descripción del riesgo se propone una estructura que facilita su redacción y claridad, como se describe a continuación:

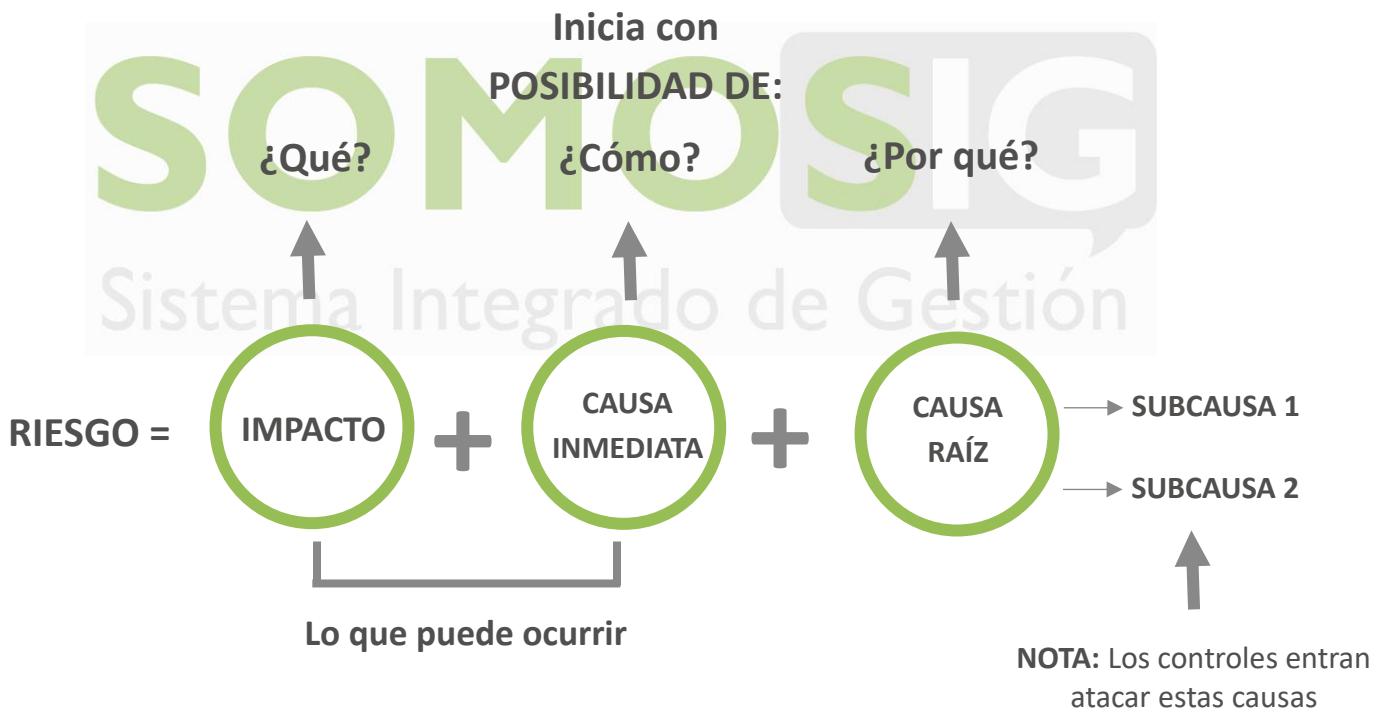

Imagen 4. *Estructura propuesta para la redacción del riesgo*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

Donde:

- Impacto: las consecuencias que puede ocasionar a la–Entidad la materialización del riesgo (Afectación económica, afectación reputacional o afectación económica y reputacional)

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

Estos dos elementos facilitan la definición del evento no deseado (¿qué podría ocurrir?), es decir, aquella situación, acción, condición o hecho incierto que, de materializarse y podría impactar el cumplimiento de los objetivos de la entidad. Este evento debe describirse de manera específica y clara, evitando formulaciones genéricas, y expresarse en términos de lo que podría suceder.
- Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para el diseño y análisis 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, al identificar causa raíz pueden agruparse en humanas, tecnológicas, normativas, ambientales u organizacionales, un análisis adecuado de la causa raíz debe permitir diferenciarla de la causa inmediata.

A continuación, se describen algunas premisas para una adecuada redacción del riesgo:

Tabla 5. *Premisas redacción del riesgo*

Descripción	Ejemplo
En la definición del riesgo se debe evitar iniciar con palabras negativas	"No…", "Que no…", o con palabras que denoten un factor de riesgo (causa) tales como: "ausencia de", "falta de", "poco(a)", "escaso(a)", "insuficiente", "deficiente", "debilidades en…"
No describir como riesgos fallas ni desviaciones del control	Errores en la liquidación de la nómina por fallas en los procedimientos existentes.
No describir causas como riesgos	Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
No describir riesgos como la negación de un control	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	El riesgo posibilidad de afectación económica y reputacional por incumplimientos a la gestión documental, debido a pérdida de expedientes en el archivo central, se encuentra asociado a la gestión documental, pero la causa raíz está relacionada con la pérdida de expedientes que puede representar un riesgo frente a la gestión contractual, la gestión jurídica entre otros y en cada proceso sus responsables y controles son específicos

Adaptada fuente: DAFP. 2025

Imagen 5. *Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

7.3 PASO 2 ANÁLISIS DE RIESGO INHERENTE

7.3.1 DETERMINAR LA PROBABILIDAD

Por probabilidad se entiende como la posibilidad de ocurrencia del riesgo, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el **número de veces que se pasa por el punto de riesgo en el periodo de 1 año**.

A continuación, se muestran ejemplos para su identificación:

Tabla 6. *Frecuencia de actividades relacionadas con la gestión*

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

Fuente: DAFP. 2025

Para su determinación se utiliza la siguiente tabla:

Tabla 7. *Criterios para definir el nivel de probabilidad*

	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 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 25 a 500 veces por año	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta más de 501 veces al año y máximo 5000 veces por año	**80%**
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5001 veces por año	**100%**

Fuente: DAFP. 2025

Nota: Si la actividad es permanente calificar la frecuencia de la actividad como muy alta y en frecuencia colocar un valor superior a 5001 veces por año.

7.3.2 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.

Para su determinación se utiliza la Tabla 8. Criterios para definir el nivel de impacto.

Tabla 8. *Criterios para definir el nivel de impacto*

	Afectación económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la entidad
Menor 40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Mayor a 51 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Mayor a 101 SMLMV y Menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 501 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: DAFP. 2025

A continuación, se presenta ejemplo aplicado de valoración de las tablas de probabilidad e impacto:

	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 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 25 a 500 veces por año	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta más de 501 veces al año y máximo 5000 veces por año	**80%**
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5001 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 entidad
Menor 40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Mayor a 51 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Mayor a 101 SMLMV y Menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 501 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 500 SMLMV, el impacto del riesgo es **mayor.**

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

Imagen 6. *Ejemplo aplicado a tablas de probabilidad e impacto.*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

7.3.3 ANÁLISIS DE SEVERIDAD

Se logra a través de la combinación de la probabilidad y el impacto como se mencionó anteriormente por medio de las tablas establecidas. Para su determinación se utiliza la Matriz de criticidad de 5x5, la cual determina que para ubicar el nivel de riesgo se cuenta con cinco niveles en probabilidad y 5 niveles en impacto, Se definen 4 zonas de severidad en la matriz de calor, como se muestra a continuación:

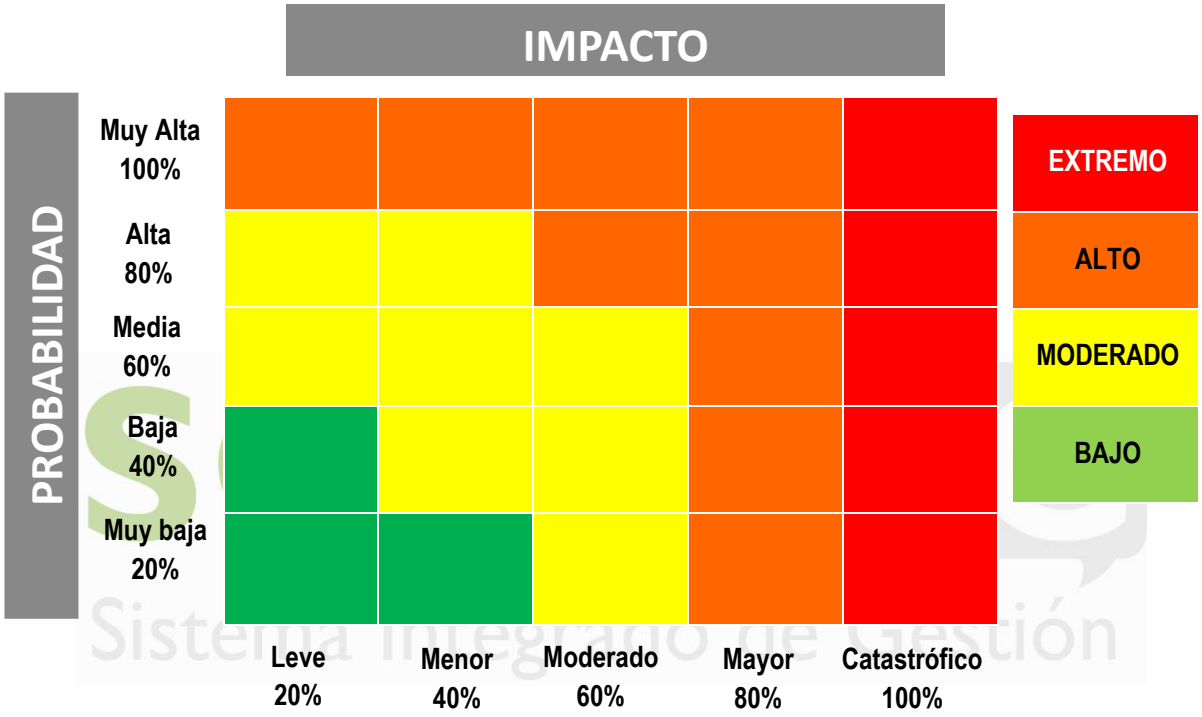

***Imagen 7**. Matriz de calor (niveles de severidad del riesgo)*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas - DAFP. 2022.

A continuación, se presenta ejemplo aplicado de determinación de nivel de severidad: **Probabilidad inherente** = media 60%, **impacto inherente:** mayor 80%

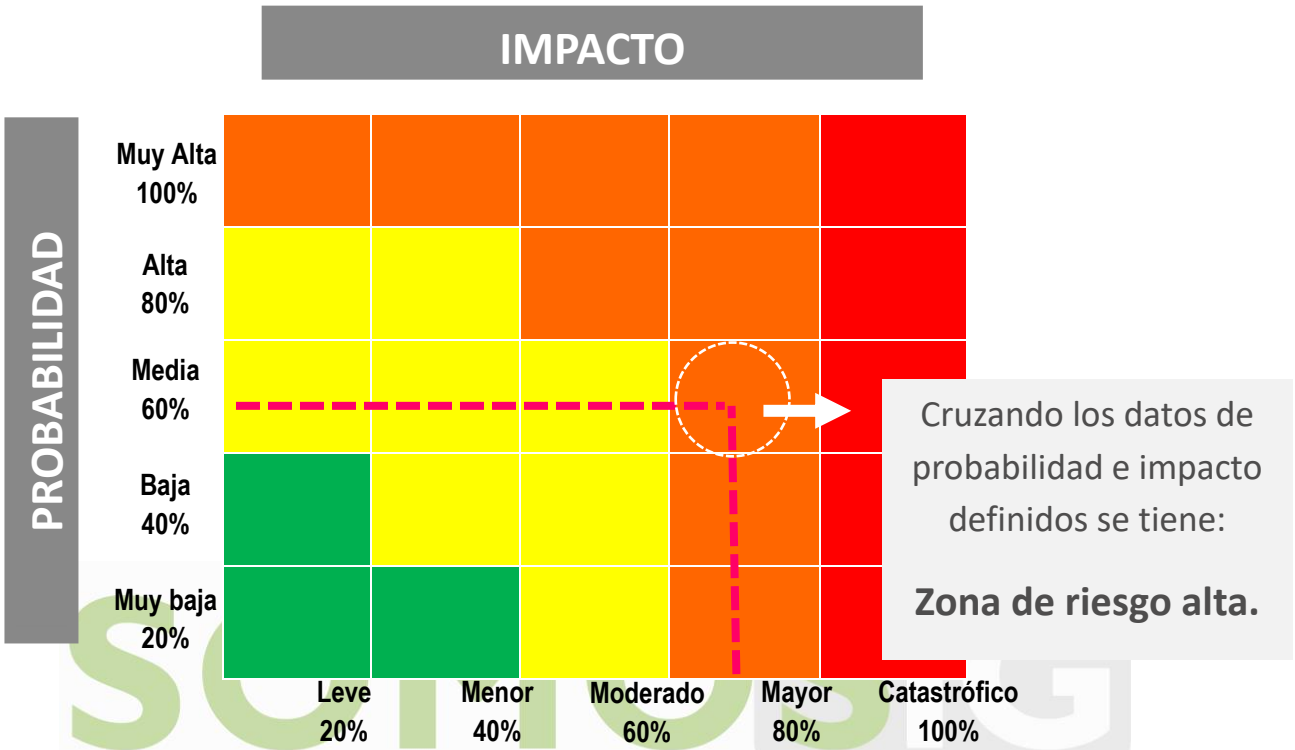

Imagen 8. *Ejemplo aplicado matriz de calor*

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se determina el nivel de riesgo inherente.

7.4 PASO 3 DISEÑO Y ANÁLISIS DE CONTROLES

7.4.1 VALORACIÓN DE CONTROLES

Se busca confrontar los resultados del análisis del riesgo inicial (INHERENTE) frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RESIDUAL).

Riesgo inicial (Inherente) – Efecto de los controles = Riesgo Final (Residual)

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

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas y factores de riesgo, que hacen que el riesgo se materialice.

Es necesario tener en cuenta los distintos atributos de las actividades de control para garantizar aspectos como la asignación de responsables, una adecuada segregación de funciones y niveles de autoridad pertinentes.

7.4.2 ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, se deberá tener en cuenta la estructura organizacional de la entidad, las distintas categorías de empleo (directivos, asesores, coordinadores, profesionales, técnicos y asistenciales) y su asignación dentro de los grupos internos de trabajo. En el caso de los controles automáticos, se deberá identificar al responsable de su calibración o parametrización periódica del sistema de información o software mediante el cual se ejecuta el control.

- Acción: Describe el propósito del control, se recomienda emplear verbos de acción que reflejen actividades de seguimiento y validación, tales como: verificar, validar, conciliar, comparar, revisar, cotejar o detectar.

- Complemento – Atributos informativos o de formalización del control: del control: corresponde a los detalles que permiten al responsable implementar el control como ha sido diseñado, contempla los siguientes aspectos:

  - Documentación: hace referencia a la fuente documental de los controles, la cual puede estar contenida en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
  - Frecuencia: periodicidad con la cual se ejecuta el control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. Su aplicación puede realizarse de forma periódica o en respuesta a eventos específicos.
  - Evidencia: registro que permiten contar con la trazabilidad en la ejecución del control. Puede ser manual o electrónico.
  - Ejecución: permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta.

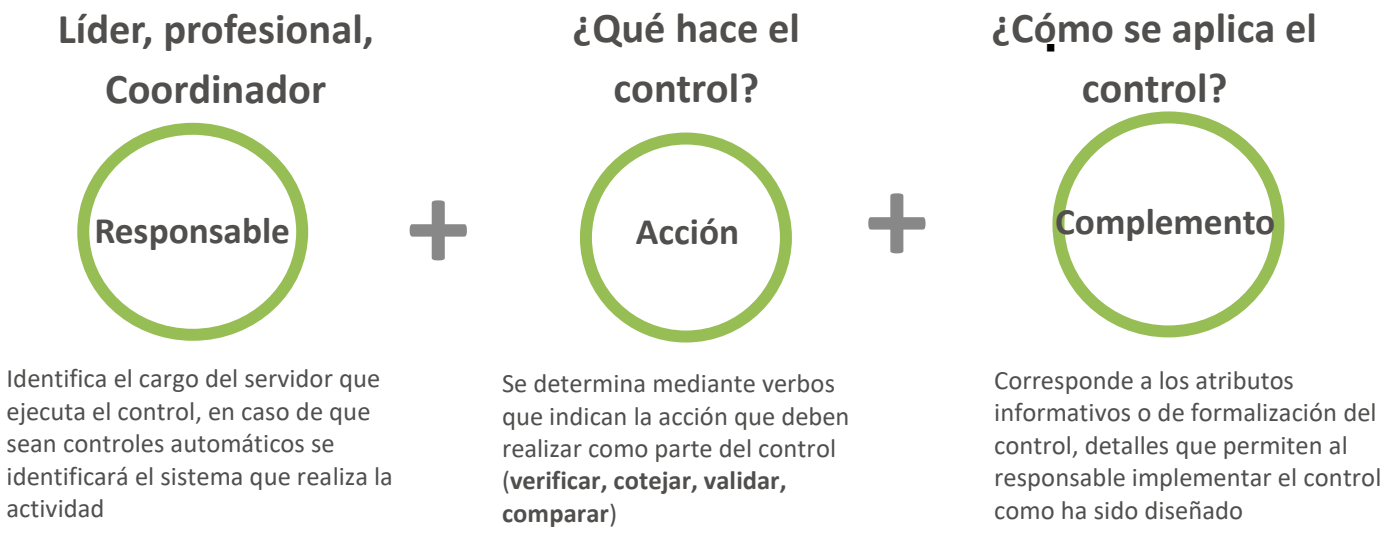

***Imagen 9**. Estructura para la redacción de controles*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

A continuación, se presenta ejemplo aplicado de la redacción del control:

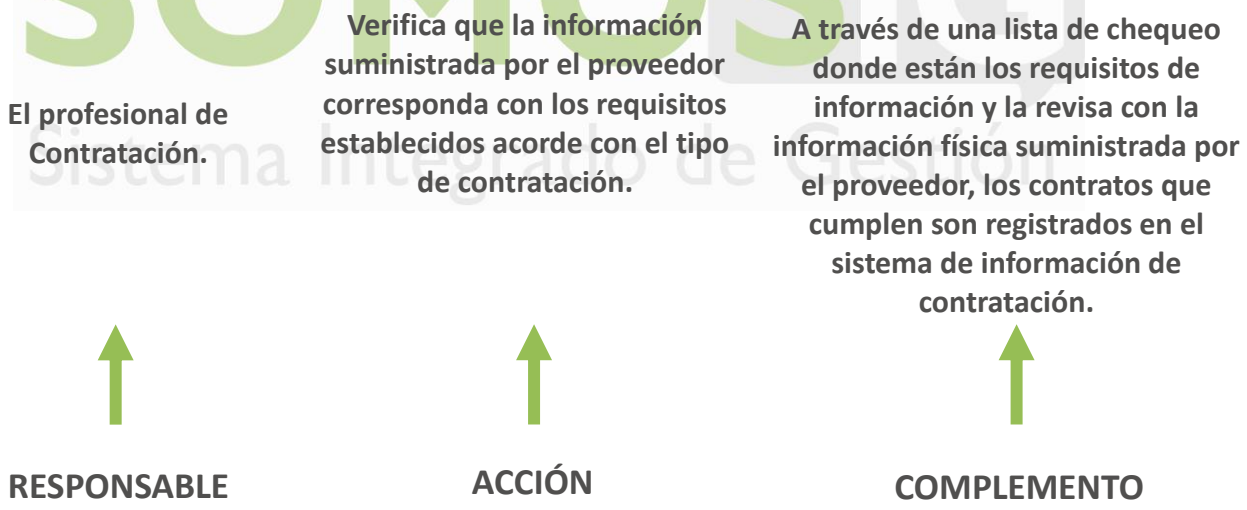

***Imagen 10.** Ejemplo aplicado redacción del control.*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

7.4.3 TIPOLOGÍAS DE CONTROLES

Es necesario analizar el ciclo de los procesos con el fin de identificar en qué momento se activa un control y, a partir de ello, determinar si corresponde a un control preventivo, detectivo, correctivo o a una combinación de estos., como se describe a continuación:

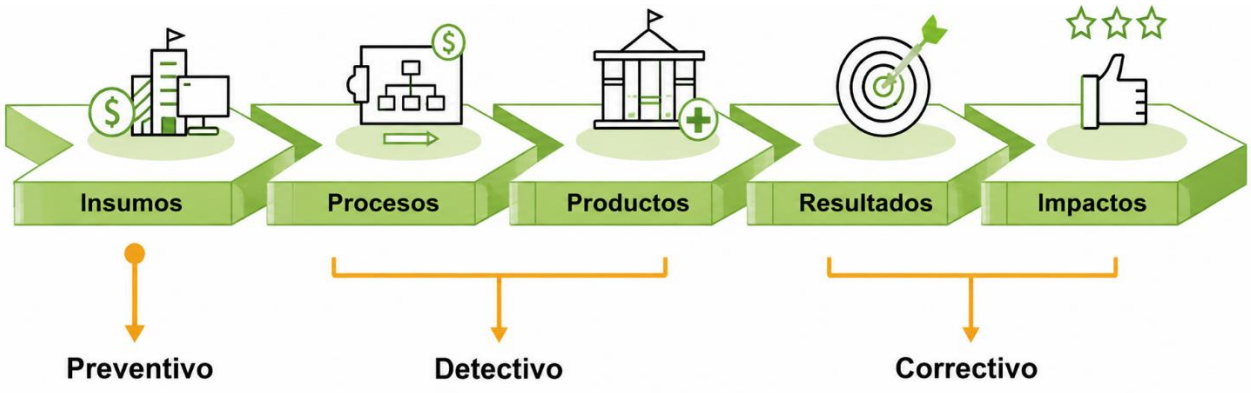

Imagen 11. *Cadena de valor del proceso y tipologías de controles.*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2025

- 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. Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo.
- Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Detecta que algo ocurre y devuelve el proceso a los controles preventivos, atacan la probabilidad de ocurrencia del riesgo.
- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Atacan el impacto frente a la materialización del riesgo. Los controles incluidos en esta tipología suelen estar asociados a pólizas de seguro, copias de seguridad (backup), bancos de datos u otros mecanismos diseñados para responder al riesgo una vez se ha materializado, los cuales se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización pero no pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad.

Así mismo, según la forma en que se ejecutan, los controles pueden clasificarse en:

- Control manual: realizado directamente por personas.

- Control automático: ejecutado por sistemas o software previamente programados o diseñados.

7.4.4 VALORACIÓN DE CONTROLES

Determina la forma como se califican los atributos o características de Eficiencia como se muestra en la tabla 9, para los atributos informativos o de formalización del control no se aplica valoración, pero se analizan para garantizar su diseño como se establece en la tabla 10:

Tabla 9. *Valoración del control*

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%

Fuente: DAFP. 2025

Tabla 10. *Análisis atributos para la formalización del control*

Características de eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
	Interna	Formatos o registros internos formales.

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

Fuente: DAFP. 2025

7.4.5 APLICACIÓN DE CONTROLES EN LA MATRIZ DE SEVERIDAD

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

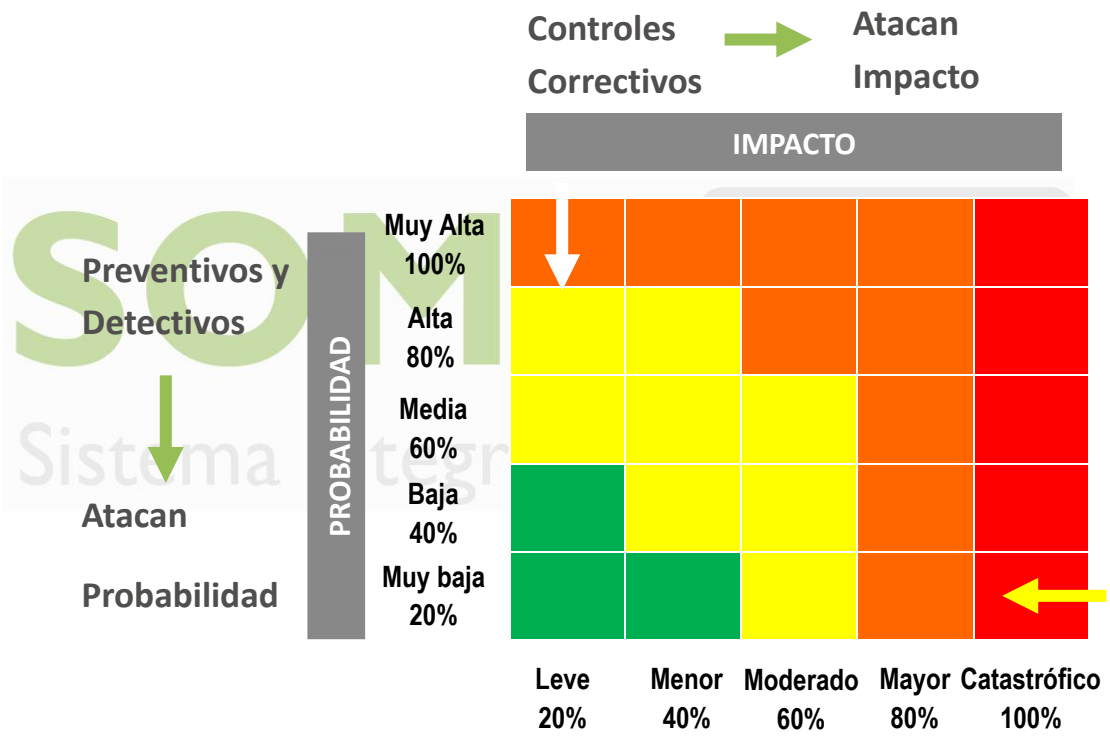

Imagen 12. *Movimiento en la matriz de calor acorde con el tipo de control.*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

7.5 PASO 4: VALORACIÓN DE RIESGO RESIDUAL

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

A continuación, se presenta ejemplo aplicado de la tabla de análisis atributos para la formalización del control:

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

Imagen 13. *Ejemplo aplicado a la tabla de análisis atributos para la formalización del control*
Fuente DAFP.2025

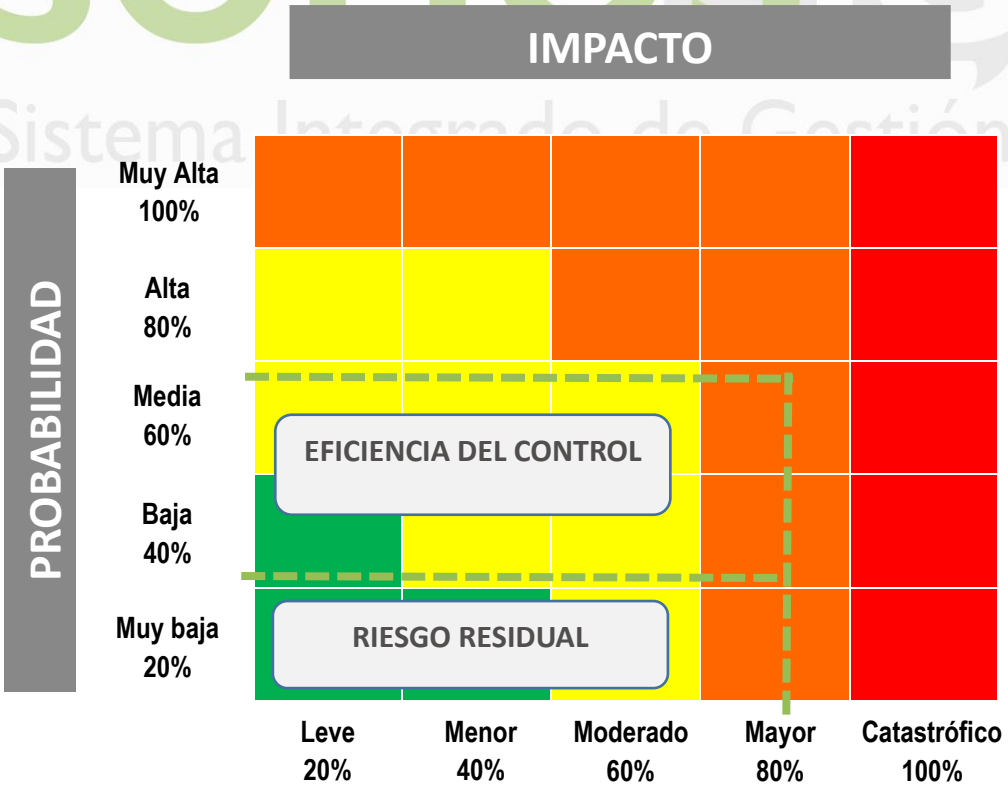

Imagen 14. *Movimiento en la matriz de calor con el ejemplo propuesto*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente.

El mapa de calor permite visualizar los riesgos en las zonas definidas (bajo, moderado, alto y extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a aceptar en función del impacto de estos en la Entidad.

Frente a las zonas de riesgo se define el siguiente tratamiento:

Zona de riesgo baja: Aceptar el riesgo.
Zona de riesgo Moderada: Reducir el riesgo.
Zona de riesgo Alta: Reducir el riesgo, evitar, transferir o compartir
Zona de riesgo Extrema: Reducir el riesgo, evitar, transferir o compartir

El tratamiento implica la selección de una o varias opciones para el manejo de los riesgos identificados, evaluados y valorados. Dentro de las opciones y luego de determinar la zona de riesgo, se pueden contemplar las siguientes:

- **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.

- **Reducir el riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es alto se determina tratarlo mediante transferencia o mitigación del riesgo.

- **Mitigar el riesgo:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

  Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001.

- **Transferir o compartir el riesgo:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas.

  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.

  La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

  Nota: Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

- **Aceptar el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Se determina asumir el riesgo conociendo lo efectos de su posible materialización. Ningún riesgo de corrupción podrá ser aceptado.

La selección de una o más opciones de tratamiento, requiere del análisis costo-beneficio, acompañado de elementos como la viabilidad jurídica, técnica e institucional de la opción u opciones a implementar y la aprobación del dueño del proceso o la dirección según sea el caso.

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

7.5.1 CONSOLIDACIÓN MAPA DE RIESGOS INTEGRAL

El mapa de riesgos institucional, se consolida en el documento soporte el cual se puede consultar en el portal WEB institucional en el enlace https://www.minambiente.gov.co/planeacion-y-seguimiento/administracion-del-riesgo

Así como, en el aplicativo del Sistema Integrado de Gestión SOMOSIG, una vez sea aprobado por los responsables de los procesos en el Comité Institucional de Gestión y Desempeño.

7.6 SEGUIMIENTO, MONITOREO Y REVISIÓN EN EL MARCO DEL ESQUEMA DE LÍNEAS DEL MODELO ESTÁNDAR DE CONTROL INTERNO MECI

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

En este contexto, los Indicadores Clave de Riesgo (*Key Risk Indicators* – KRI por sus siglas en inglés), surgen como una herramienta fundamental para la toma de decisiones informadas de cara a la mitigación de riesgos.

7.6.1 INDICADORES PARA EL SEGUIMIENTO

Con el propósito de definir de forma adecuada los Indicadores Clave de Riesgo, es necesario enmarcarlos desde la plataforma estratégica de la entidad y su despliegue en los objetivos estratégicos y de los procesos, constituyéndose en la base para la identificación y formulación de Indicadores Clave de Desempeño *(Key Performance Indicators – KPI),* que hacen posible medir su cumplimiento. En este sentido, se vinculan los Indicadores clave de riesgo articulados con los Indicadores clave de proceso del Sistema Integrado de Gestión.

Imagen 15. *Articulación Indicadores Clave de Riesgo y los Indicadores Clave de Proceso*
Fuente: Adaptado documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

En consecuencia, los indicadores tienen una función principal que es monitorear los riesgos clave que podrían afectar el cumplimiento de los objetivos y metas establecidos durante las diversas etapas de la gestión institucional.

7.6.2 ALCANCE DE LOS INDICADORES CLAVE DE PROCESO (KPI) Y LOS INDICADORES CLAVE DE RIESGO (KRI)

Los alcances en la aplicación de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI), son complementarios en su análisis al tener objetivos y/o características diferentes así:

Tabla 11. *Alcance aplicación KPI y KRI*

Indicadores Clave de Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
Permiten medir periódicamente el desempeño general de la entidad y sus principales unidades operativas.	Complementan el seguimiento a los resultados de la entidad.
Se definen tomando como referencia las metas establecidas, por procesos, unidades u operaciones clave.	Proporcionan una señal temprana y oportuna de una exposición al riesgo en diversas áreas de la entidad.
Mide el rendimiento pasado, proporcionando información sobre qué tan bien se están logrando los objetivos estratégicos y operativos.	Proporcionan información útil sobre los riesgos emergentes y potenciales que pueden impactar en los objetivos estratégicos de la organización.

Indicadores Clave de Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
Ofrecen información sobre aquellos aspectos críticos de la operación que requieren mayores recursos y atención.	Ayudan a identificar y anticipar problemas que se pueden presentar interna o externamente, así como oportunidades futuras.
Permiten medir los resultados que se obtienen de la ejecución de los programas, planes y proyectos, en los diferentes momentos o etapas de su desarrollo.	Permiten realizar un monitoreo constante y mitigar los posibles eventos de riesgo que se presenten al aplicar medidas oportunas para disminuir su impacto.
Permiten mejorar la planificación, entender con mayor precisión las oportunidades de mejora de determinados procesos y analizar el desempeño de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad.	Facilitan el proceso de generación de informes y el escalamiento de los riesgos.

Los Indicadores Clave de Riesgos (*KRI*), hacen referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No necesariamente indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe analizar.

Estos indicadores permiten registrar la ocurrencia de un evento que se asocia a un riesgo identificado previamente, lo cual permite llevar un registro de eventos y evaluar a través de su tendencia la efectividad de los controles que se disponen para mitigarlos. A continuación, se presentan algunos ejemplos:

Tabla 12. *Ejemplos indicadores clave de riesgo*

Proceso Asociado	INDICADOR	MÉTRICA
Gestión de servicios de información y soporte tecnológico	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
Gestión Financiera	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
Servicio al Ciudadano	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
Administración del Talento Humano	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

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

En el Ministerio de Ambiente y Desarrollo Sostenible, se formularán indicadores claves de riesgo – KRI, a los riesgos que se encuentren en zona de severidad extrema después de la valoración del riesgo residual en el

módulo de riesgos del aplicativo SOMOSIG, para el seguimiento y monitoreo de los riesgos, ya que pueden entregar señales de alerta temprana, así como detectar tendencias o cambios en los niveles de riesgo, lo que facilita que se incorporen acciones correctivas y preventivas para minimizar sus impactos frente a posibles materializaciones.

7.6.3 MONITOREO Y REVISIÓN

El monitoreo y revisión tiene como propósito valorar la efectividad de los controles establecidos por la entidad, el nivel de ejecución de los planes de manejo o tratamiento de los riesgos que permiten asegurar los resultados de la gestión, así como detectar las desviaciones y tendencias para generar recomendaciones sobre el mejoramiento de los procesos, y determinar si existen cambios en el contexto interno o externo, incluyendo los cambios en los criterios de riesgo y en el propio riesgo.

Responsables de los procesos

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión de "Control Interno", del Modelo Integrado de Planeación y Gestión – MIPG, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad en el marco de las líneas de defensa así (Fuente: Manual MIPG)

Línea Estratégica: Define el marco general para la gestión del riesgo y el control, mediante el establecimiento de la política de administración del riesgo. Conformada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno.

1era línea de defensa: La gestión operacional se encarga de desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, evaluación, control y mitigación. A cargo de los gerentes públicos y líderes de los **procesos**, programas y proyectos de la entidad. Tiene como rol principal: diseñar, implementar los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

De acuerdo con lo anterior, cada líder de proceso debe mantener la traza o documentación respectiva de todas las actividades realizadas que garanticen de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplan.

2da línea de defensa: Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. Ocupados por cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos,

coordinadores de sistemas de gestión de la Entidad, líderes o coordinadores de contratación, financiera y de TIC, entre otros.

El rol principal es monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo, así como, el aseguramiento sobre el diseño apropiado de los controles, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica)

3ra línea de defensa: A cargo de la Oficina de Control Interno, auditoría interna o quien haga sus veces. El rol principal es proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno.

El alcance de este aseguramiento se realiza a través de la auditoría interna que cubre todos los componentes del Sistema de Control Interno. Evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos o inadecuadamente cubiertos por la 2ª línea de defensa.

Las interacciones entre la 2ª línea de defensa (proveedores internos de aseguramiento) y la 3ª línea de defensa y estas con los proveedores externos de aseguramiento (organismos de control y otras instancias de supervisión o vigilancia) son representadas en el mapa de aseguramiento, herramienta que permite coordinar las diferentes actividades de aseguramiento, visualizar el esfuerzo en común y mitigar los riesgos de una manera mucho más integral. Adicionalmente, tiene como roles el liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento.

Tabla 12. *Responsabilidad frente a la gestión del riesgo*

Línea	Responsable	Responsabilidades
Línea Estratégica	Alta Dirección	● Analizar los riesgos y amenazas institucionales frente al cumplimiento de los planes estratégicos (objetivos, metas, indicadores). ● Aprobación de la política de administración del riesgo, la asignación de recursos y responsabilidades para su implementación ● Definición del apetito de riesgo
	Comité Institucional de Coordinación de Control Interno	● Definir el marco general, roles y responsabilidades para la gestión del riesgo (política de administración del riesgo) y el control de riesgos. ● Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
		● Identificar cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos.
		● Revisar que los riesgos identificados tengan el impacto en el cumplimiento de objetivos estratégicos, estén alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos.
		● Revisar y tomar decisiones frente a los riesgos materializados con el fin de evitar su repetición.
		● Realizar el análisis de eventos y riesgos críticos que tienen un nivel de severidad muy alto frente a los cuales se deben tomar decisiones.
		● Hacer seguimiento a los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna frente a la administración de riesgos.

Línea	Responsable	Responsabilidades
		● Servir de instancia para resolver las diferencias que surjan en desarrollo del ejercicio de auditoría interna. ● Conocer y resolver los conflictos de interés que afecten la independencia de la auditoría
		● Analizar los cambios en el entorno interno y externo que puedan tener un impacto significativo en la entidad y que puedan generar cambios en la estructura de riesgos y controles.
		● Revisar los informes presentados de los eventos de riesgos que se han materializado en la entidad, así como las causas que dieron origen a esos eventos.
		● Hacer seguimiento y pronunciarse sobre el perfil de riesgo inherente y residual de la entidad y de acuerdo con las políticas de tolerancia, establecidas y aprobadas. ● Evaluar el estado del Sistema de Control Interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del sistema con enfoque preventivo ● Aprobar el Plan Anual de Auditoría de la entidad, hacer sugerencias y seguimiento a las recomendaciones, con el fin de asegurar que su alcance y recursos faciliten la cobertura de los proyectos estratégicos de la entidad, así como, la priorización de las unidades auditables críticas para la misma, según la priorización y el análisis de riesgos hecho por la Oficina de Control Interno y/o quien haga sus veces. ● Verificar que el esquema de líneas atiende de manera íntegra la gestión del riesgo al interior de la entidad, comprometiendo todos los niveles de la organización
	Comité Institucional de Gestión y Desempeño	● Aprobar el mapa de riesgos actualizado para cada vigencia. ● Aprobar y hacer seguimiento a las acciones y estrategias adoptadas para la operación del MIPG ● Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del MIPG ● Incorporar dentro de la planeación estratégica el análisis de riesgos para decidir respecto de los objetivos, las metas y niveles de riesgo aceptados y no aceptados en su consecución. ● Adelantar y promover acciones permanentes de autodiagnóstico, estableciendo los mecanismos y responsables de monitorear el desempeño los resultados de la gestión de riesgos. ● Compartir los resultados de la gestión del riesgo, monitoreo y seguimiento del mapa de riesgos institucional, para la definición de las acciones estratégicas y/o o de mejora. ● Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando.
1ª Línea de defensa	Jefes de área o líderes de proceso, facilitadores y sus equipos de trabajo.	● Implementar la G-E-SIG-05 "Guía para la Gestión Integral del Riesgo".
		● Implementar y mantener los controles establecidos en el mapa y plan de manejo de riesgos.
		● Implementar acciones correctivas en los casos que se detecten deficiencias del control.
		● Revisar los cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos de los procesos y actualizar la matriz F-E-SIG-28 mapa de riesgos institucional.
		● Revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
		● Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.

Línea	Responsable	Responsabilidades
		● Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
		● Revisar y reportar a la Oficina Asesora de Planeación, los riesgos que se han materializado, así como, las causas que dieron origen a esos eventos.
		● Revisar las acciones formuladas para cada uno de los riesgos materializados con el fin de tomar medidas para evitar su repetición y lograr el cumplimiento a los objetivos.
		● Revisar y hacer seguimiento al cumplimiento de las actividades y planes de manejo aprobados, con relación a la gestión de riesgos.
		● Reportar oportunamente el avance de las acciones del plan de manejo e implementación de controles del mapa de riesgos del proceso de los cuales es responsable y proponer proactivamente mejoras en los mismos cuando sean necesarias
2ª Línea de defensa	Responsables del monitoreo y evaluación de controles y gestión del riesgo: jefe de la Oficina Asesora de Planeación a través del grupo de Gestión y Desempeño Institucional - GDI, coordinadores de equipos de trabajo, supervisores de contratos, Comité de contratación, áreas financieras y responsables de sistemas de gestión.	● Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de defensa sean apropiados y funcionen correctamente y determina las recomendaciones para el fortalecimiento de estos.
		● Ejerce el control y la gestión de riesgos, las funciones de cumplimiento, seguridad y calidad.
		● Supervisa la implementación de prácticas de gestión de riesgo eficaces por parte de la primera línea y ayuda a los responsables de riesgos a distribuir información adecuada sobre riesgos a todos los servidores del Ministerio.
		● Revisar los cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos de los procesos con el fin de solicitar y apoyar en la actualización de la matriz F-E-SIG-28 mapa de riesgos institucional.
		● Revisar que los riesgos identificados tengan el impacto en el cumplimiento de objetivos estratégicos, estén alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos y realizar las recomendaciones a que haya lugar.
		● Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
		● Consolidar el mapa de riesgos institucional, priorizando el análisis de aquellos riesgos de mayor criticidad que puedan afectar el cumplimiento de los objetivos institucionales y presentarlo semestralmente ante la línea estratégica para su análisis y toma de decisiones correspondiente
		● Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
		● Revisar los riesgos materializados con el fin de tomar medidas para evitar su repetición y lograr el cumplimiento a los objetivos.
		● Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de defensa sean apropiados y funcionen correctamente y determina las recomendaciones para el fortalecimiento de estos.
3ª Línea de defensa	Oficina de Control Interno	● Proporcionar información sobre la efectividad del Sistema de Control Interno, la operación de la primera y segunda línea de defensa con un enfoque basado en riesgos.
		● La función de auditoría interna, a través de un enfoque basado en el riesgo, proporciona aseguramiento sobre la eficacia institucional, gestión de riesgos y control interno a la Alta Dirección, incluyendo el funcionamiento de la primera y segunda línea de defensa.
		● Revisar los cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos de los procesos, con el fin de que se identifique y actualice la matriz F-E-SIG-28 mapa de riesgos institucional por parte de los responsables.

Línea	Responsable	Responsabilidades
		● Revisar que los riesgos identificados tengan el impacto en el cumplimiento de objetivos estratégicos, estén alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos y realizar las recomendaciones a que haya lugar.
		● Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
		● Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.
		● Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
		● Para mitigar los riesgos de los procesos revisar que se encuentren documentados y actualizados los procedimientos y los planes de mejoramiento resultado de las auditorías efectuadas; que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.
		● Informar sobre las auditorías basadas en riesgos, que se ejecuten con énfasis en riesgos fiscales.

Adaptada Fuente: DAFP. 2018

La Oficina de Tecnologías de la Información y la Comunicación – OTIC liderará el proceso de formulación y monitoreo de los riesgos de seguridad de la información del Ministerio, formulación que una vez aprobada por los líderes de proceso y el Comité Institucional de Gestión y Desempeño, será consolidada en el mapa de riesgos institucional por parte de la Oficina Asesora de Planeación. Este ejercicio se articulará con el cronograma de actualización de los riesgos de gestión y corrupción para cada vigencia, liderado por la Oficina Asesora de Planeación.

Corresponde a la Oficina de Tecnologías de la Información y la Comunicación – OTIC, realizar el acompañamiento técnico a las dependencias para que ellas puedan atender las observaciones, hallazgos o recomendaciones que realice la Oficina de Control Interno, entes reguladores o cualquier otra instancia, frente a los riesgos de seguridad de la información del Ministerio y la efectividad de los controles implementados, como líder del Modelo de Seguridad y Privacidad de la Información – MSPI.

Los riesgos se actualizan y validan de manera permanente y en cualquier momento de ser necesario, considerando las condiciones de operación internas o externas. Cada líder de proceso actualiza el análisis de contexto, riesgos y controles como resultado de los ejercicios de autocontrol, autoevaluación, evaluación independiente o por decisión del Comité Institucional de Coordinación de Control Interno, según estime conveniente para asegurar el cumplimiento de los objetivos del proceso.

En todo caso la revisión y actualización se realizará mínimo una vez al año con el acompañamiento de la Oficina Asesora de Planeación, la Oficina TIC según el tipo de riesgo y la asesoría de la Oficina de Control Interno.

La fecha programada para el cumplimiento de las acciones del mapa de riesgos aprobado, será hasta el primer trimestre de la siguiente vigencia, con el fin realizar el seguimiento y monitoreo del cierre de la gestión.

De otra parte y en concordancia con "La Guía para la Gestión del riesgo de Corrupción" de la Presidencia de la República, los riesgos de corrupción actualizados se publican a más tardar el 31 de enero de cada año, se realizarán seguimientos periódicos sobre los posibles actos de corrupción mediante la evaluación de los riesgos de corrupción, equiparando dicho seguimiento a las fechas establecidas de seguimiento al Plan Anticorrupción y atención al ciudadano ahora Programa de Transparencia y Ética Pública, las cuales son 3 veces al año empezando el 1ero con corte al 30 de abril, el 2do con corte al 31 de agosto y el 3ero con corte al 31 de diciembre.

Dicho seguimiento se publicará en la página web de la entidad o en lugar de fácil acceso al ciudadano.

Se puede considerar la eliminación de los riesgos que se encuentren en nivel de aceptación Bajo o aceptable, los cuales deberán soportar la evidencia de la implementación de sus controles existentes de manera que justifiquen la no materialización durante la vigencia.

El responsable de cada proceso registra dos veces en el año en el mapa de riesgos o de acuerdo con las solicitudes de monitoreo de la Oficina Asesora de Planeación, el estado de la gestión de las acciones y controles formulados junto con las evidencias correspondientes, describiendo concretamente si hubo o no riesgos materializados, así mismo, se deberá analizar el cumplimiento de los indicadores de gestión y su relación con la materialización de los riesgos.

Si se identifican riesgos materializados por cualquiera de las líneas de defensa, de manera inmediata se ejecutan las acciones para su tratamiento.

7.6.4 RIESGOS MATERIALIZADOS

Cuando se detecte la materialización de los riesgos, s se realizarán las siguientes acciones:

a) Materialización de riesgos detectada por parte del líder del proceso (primera línea de defensa):

- Cuando se identifiquen hechos, situaciones o eventos asociados a riesgos de integridad pública (SIGRIP), corrupción, lavado de activos, financiación del terrorismo y de la proliferación de armas de destrucción masiva (LA/FT/FPADM), soborno o fraude, se deberá informar de manera inmediata a la Oficina Asesora de Planeación, en su calidad de representante de la Alta Dirección para el Sistema Integrado de Gestión, de conformidad con lo establecido en la Resolución 2140 de 2017, para la evaluación y gestión correspondiente.

  Adicionalmente, y en cumplimiento de lo dispuesto en la Directiva Presidencial No. 01 de 2015, el hecho deberá ser puesto en conocimiento del Jefe de la Oficina de Control Interno, con el fin de que adelante las actuaciones de su competencia y, cuando corresponda, efectúe el reporte a la Secretaría de Transparencia de la Presidencia de la República. Sin perjuicio de lo anterior, cuando la naturaleza de los hechos lo amerite, se deberán realizar las denuncias o reportes ante las autoridades u organismos de control competentes.

- Si el riesgo es de gestión, se deberá realizar el análisis de causas y determinar acciones, análisis y actualización del mapa de riesgos.

b) Materialización de riesgos detectada por la segunda línea de defensa:

- En los casos de riesgos de corrupción detectado por la segunda Línea de defensa, se debe:
  - Informar sobre el hecho encontrado a la Oficina de Control Interno, para lo de su competencia
  - Informar al líder del proceso, para revisar el mapa de riesgos y sus controles asociados, verificar que se tomaron las acciones y que se actualizó el mapa de riesgos.

- En los casos de riesgos de Gestión detectado por la segunda Línea de defensa, se debe comunicar a la Oficina de Control Interno, para lo de su competencia y al líder del proceso sobre el hecho encontrado, para que realice la revisión, análisis y acciones correspondientes para resolver el hecho y verificar que se tomaron las acciones, que se actualizó el mapa de riesgos correspondiente e informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

c) Materialización de riesgos detectada por parte de la Oficina de Control Interno (tercera línea de defensa):

- Si el riesgo es de corrupción, se deberá convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. Verificar si se tomaron las acciones y si se actualizó el mapa de riesgos.

- Si el riesgo es de gestión, informar al líder del proceso sobre el hecho encontrado y orientarlo frente a la revisión, análisis y acciones correspondientes para resolver el hecho. Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada.

SOMOSIG Sistema Integrado de Gestión

8 COMUNICACIÓN Y CONSULTA

La comunicación y la consulta deberán surtirse en todas las etapas de construcción del mapa de riesgos institucional en el marco de un proceso participativo que involucre actores internos y externos del ministerio.

Esta etapa tiene como principales objetivos los siguientes:

1. Ayudar a establecer el contexto estratégico
2. Ayudar a determinar que los riesgos estén correctamente identificados.
3. Reunir diferentes áreas de experticias para el análisis de los riesgos.
4. Fomentar la gestión de riesgos.

Una vez surtido este proceso de consulta es de suma importancia que se comunique internamente el mapa de riesgos institucional y externamente el mapa de riesgos de corrupción. De tal manera que funcionarios y contratistas del ministerio; así como las partes interesadas, conozcan la forma como se estructuran los riesgos de gestión y corrupción.

CAPITULO II. GESTIÓN PREVENTIVA DE RIESGOS FISCALES

9 ARTICULACIÓN MODELO CONSTITUCIONAL CONTROL FISCAL Y SISTEMA DE CONTROL INTERNO

La Gestión del Riesgo Fiscal, tiene como finalidad orientar el análisis de la operación de las entidades públicas para identificar y gestionar los riesgos que puedan provocar un daño patrimonial al Estado, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado.

La articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), se define como un modelo de control fiscal multinivel. El Control Fiscal Interno (CFI) se entiende como el primer nivel para la vigilancia fiscal de los recursos públicos, la prevención de riesgos fiscales y la defensa del patrimonio público. El Control Fiscal Interno hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y es evaluado por la Contraloría respectiva. En la siguiente figura se visualiza la articulación del control fiscal y Sistema de Control Interno

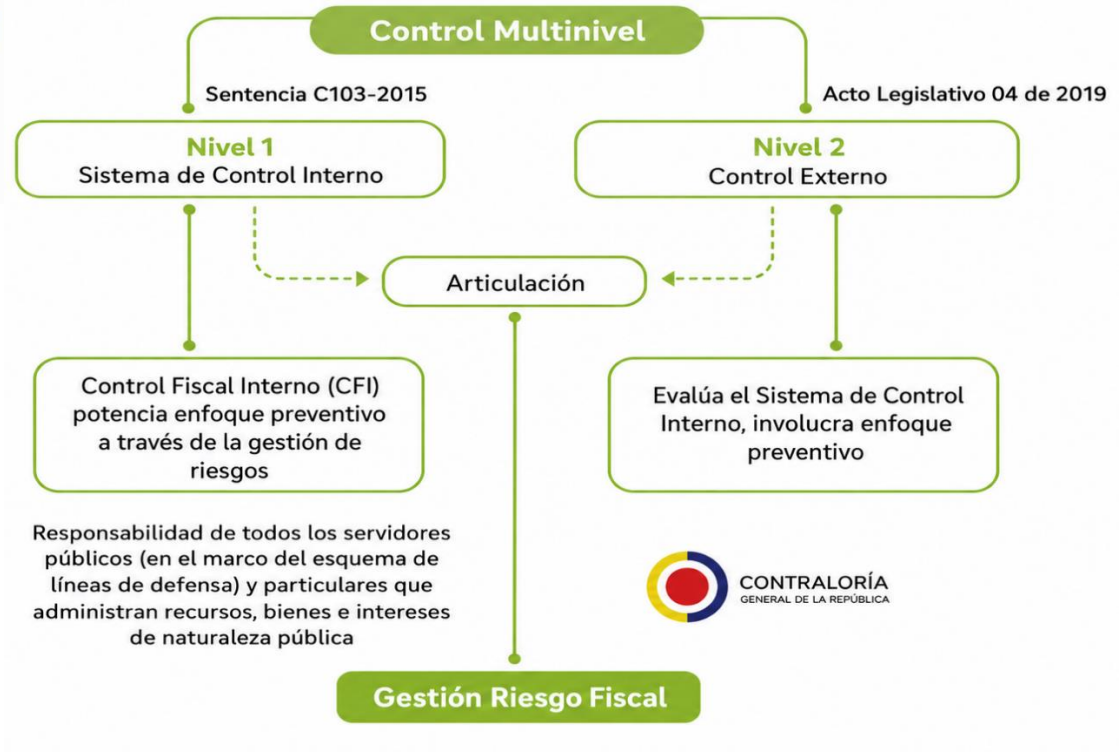

Imagen 16. *Articulación del Control Fiscal y Sistema de Control Interno*
Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Los riesgos fiscales deben ser gestionados en conjunto con los riesgos generales de gestión, riesgos de

integridad pública y los riesgos de seguridad de la información. En consecuencia, se aplicará la misma metodología, y en este aparte de la guía se hará referencia únicamente a particularidades que pueden contribuir dar mayor claridad o especificidad.

Antes de iniciar se debe recordar:

El riesgo fiscal se define así: Efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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

9.1 PASO 1 IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

Para la identificación del riesgo fiscal es necesario tener en cuenta los siguientes pasos

9.1.1 PASOS PARA LA IDENTIFICACIÓN DEL RIESGO FISCAL

Imagen 17. *Pasos para la identificación del riesgo fiscal*
Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

9.1.2 PUNTOS DE RIESGO Y LAS CIRCUNSTANCIAS INMEDIATAS

Los puntos de riesgo fiscal son eventos en los que potencialmente se genera riesgo fiscal, es decir, son las actividades propias de la gestión fiscal, para lo cual es pertinente prestar especial atención a aquellas en las cuales se han generado para el Ministerio, advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal.

Las circunstancias inmediatas son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo. Por cada punto de riesgo, con frecuencia existen múltiples

circunstancias inmediatas.

Tabla 13. *Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas*

No	Puntos de Riesgo Fiscal ***Actividad en la que potencialmente se origina el riesgo fiscal***	Circunstancia Inmediata ***Situación por la que se presenta el riesgo***
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual

No	Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal*	Circunstancia Inmediata *Situación por la que se presenta el riesgo*
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento

No	Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal*	Circunstancia Inmediata *Situación por la que se presenta el riesgo*
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
44	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
45	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
46	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
47	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
50	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
51	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2022

Nota: Los Controles de Advertencia emitidos por la Contraloría General de la República constituyen una fuente de información relevante para la identificación y análisis de posibles escenarios de riesgo fiscal; sin embargo, no generan de manera automática la incorporación de riesgos al mapa institucional. En aquellos casos en que los asuntos advertidos se relacionen con temas propios de la misionalidad de la entidad, programas, proyectos, políticas públicas, recursos naturales, bienes públicos o demás competencias institucionales que no se encuentren expresamente contemplados en el catálogo de riesgos, los líderes de proceso deberán realizar el análisis correspondiente para determinar la existencia de escenarios de riesgo fiscal asociados.

Como resultado de dicho análisis, podrán identificarse y documentarse riesgos fiscales adicionales a los establecidos en el catálogo institucional, siempre que exista la posibilidad de afectación a recursos públicos, bienes o intereses patrimoniales de naturaleza pública, de conformidad con los lineamientos definidos por el Departamento Administrativo de la Función Pública – DAFP para la gestión integral de riesgos fiscales.

Para este ejercicio, se sugieren las siguientes preguntas orientadoras para identificar puntos de riesgo fiscal y circunstancias inmediatas

Tabla 14. *Preguntas orientadoras identificación riesgo fiscal*

<table>
<tr><th>Preguntas y criterios para la identificación</th><th>Sirve para identificar</th></tr>
<tr><td>¿En qué procesos de la entidad se realiza gestión fiscal? Gestión fiscal, incluye los siguientes componentes.
</td><td>Puntos de riesgo fiscal</td></tr>
<tr><td>Qué puntos de riesgo fiscal y circunstancias inmediatas del “¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” son aplicables a la entidad?</td><td>Puntos de riesgo fiscal y circunstancias inmediatas</td></tr>
<tr><td>Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-.

Nota 1: Consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.

Nota 2: Consultar la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.

Nota 3: Los fallos con responsabilidad fiscal en firme son información pública muy importante para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o</td><td>Puntos de riesgo fiscal y circunstancias inmediatas</td></tr>
</table>

Preguntas y criterios para la identificación	Sirve para identificar
intereses patrimoniales del Estado. Nota 4: Corresponde a la segunda línea de defensa, Oficinas de Planeación con la asesoría de la Oficina de Control Interno, consultar la información y orientar a los procesos	
¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, excepto que la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.	Circunstancias inmediatas

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional, 2025

9.1.3 IDENTIFICAR EL ÁREA DE IMPACTO

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

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

Bienes públicos: Son todos aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público (aquellos cuyo uso pertenece a todos los habitantes del territorio nacional)

Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos.

Recursos públicos: Son los dineros comprometidos y ejecutados en ejercicio de la función pública. Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

9.1.4 IDENTIFICAR EL EFECTO ECONOMICO

El efecto económico del riesgo fiscal es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público. Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

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

(ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público

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

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

(v) Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.

(vi) Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su "normal uso" (máquinas eléctricas, computadores, celulares, etc.). (Contraloría General de la República, 2023, p. 12)

9.1.5 IDENTIFICAR LA CAUSA RAIZ O POTENCIAL HECHO GENERADOR

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

DESCRIPCIÓN DEL RIESGO FISCAL

La estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos. Para redactar un riesgo fiscal, se debe tener en cuenta:

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

✓ **Impacto:** corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre el área de impacto (recursos públicos, bienes o intereses patrimoniales de naturaleza pública).

✓ **Circunstancia inmediata**: corresponde al cómo. Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera.

✓ **Causa Raíz**: corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño. Es la condición necesaria del riesgo, de tal forma que, si ese hecho no se produce, el daño no se genera.

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

Redacción Inicia con:	¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de	efecto dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la inexistencia de procedimientos documentados para el ingreso y salida de bienes del almacén
	efecto dañoso sobre **recursos públicos**	por sobrecostos en contratos de la entidad	a causa de la omisión del deber de elaborar estudios de mercado
	efecto dañoso sobre **intereses patrimoniales de naturaleza pública**	por negación del reconocimiento de siniestros en el contrato de seguro	a causa de la omisión en la actualización del inventario de bienes amparados
	IMPACTO	CAUSA INMEDIATA	CAUSA RAÍZ

Imagen 18. *Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo fiscal*
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2022.

Tabla 15. *Ejemplos acorde con el objeto sobre el que recae el efecto dañoso*

Bienes Públicos	Recursos Públicos	Intereses Patrimoniales de Recursos Públicos
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la implementación y operación de redes eléctricas seguras	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por menores ingresos percibidos sobre la explotación de marcas de propiedad comercial de la entidad a causa de errores u omisiones en el análisis técnico, jurídico y económico del mercado
Posibilidad de efecto dañoso sobre bienes públicos, por deterioro en equipos técnicos a causa de la inexistencia de mantenimiento preventivo o correctivo	Posibilidad de efecto dañoso sobre los recursos de la entidad por la generación de intereses moratorios en contrato de arrendamiento a causa de la omisión en el pago oportuno del canon pactado.	Posibilidad de efecto dañoso sobre los intereses patrimoniales por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo

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

9.2 PASO 2: ANÁLISIS RIESGO INHERENTE

Se aplica la metodología sin ningún aspecto especifico. Excepto el Impacto siempre será económico

9.3 PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES

No hay nada específico frente a la metodología para la gestión integral del riesgo

9.4 PASO 4: VALORACIÓN DE RIESGO RESIDUAL

No hay nada específico frente a la metodología para la gestión integral del riesgo

SOMOSIG
Sistema Integrado de Gestión

CAPÍTULO III SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA -SIGRIP

10 SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA

En cumplimiento de la Ley 2195 de 2022, que hace obligatorio para las entidades públicas la "prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional" (artículo 31), el Ministerio de Ambiente y Desarrollo Sostenible implementa de manera articulada el Programa de Transparencia y Ética Pública con el Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP, el cual está estructurado, así:

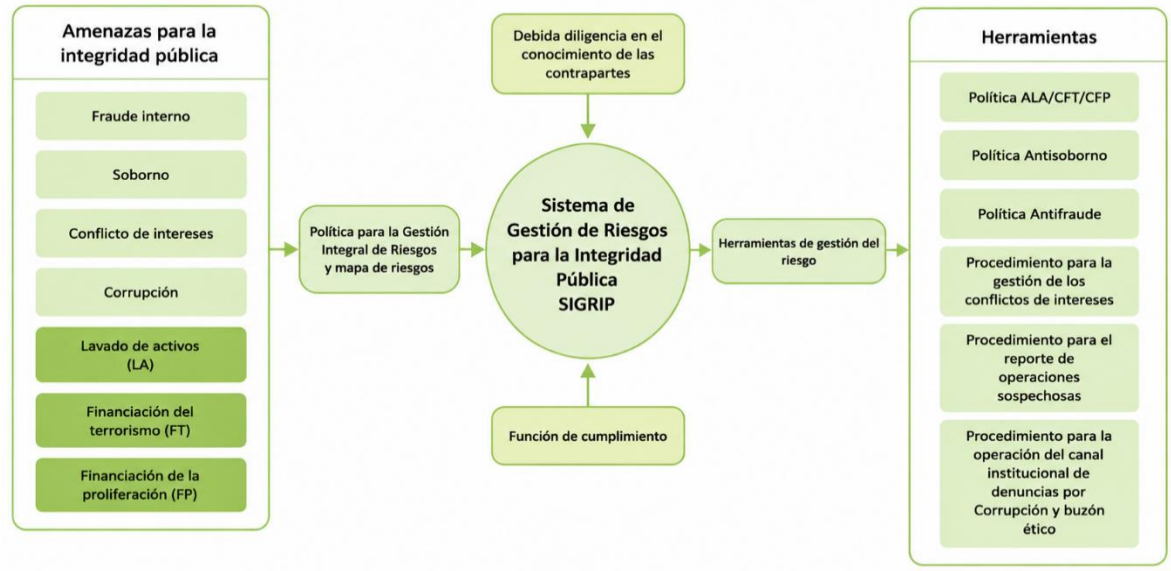

Imagen 19. *Estructura Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP*
Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Los intereses particulares, afectan la capacidad de las entidades públicas para cumplir con las funciones que se le han encomendado. En este contexto, es donde toma especial relevancia el concepto de integridad, que parte de la posibilidad de que una persona, se adecue a una serie de códigos de conducta ética preestablecidos. En esa medida, es posible promover una cultura de integridad entre los colaboradores, que privilegien el interés general del Estado en todas las decisiones que deben tomar en el ejercicio de sus funciones o del servicio que prestan.

10.1 AMENAZAS PARA LA INTEGRIDAD PÚBLICA

Para el propósito de esta guía, tomaremos las cinco amenazas para la integridad, señalados en la Guía para la Gestión Integral del Riesgo versión 7 – DAFP.

Tabla 16. *Amenazas para la Integridad Pública*

Amenazas	Descripción
Soborno	El Soborno puede ser entendido como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]. Y opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.
Fraude	El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima. El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.
Corrupción	La Corrupción es "todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral"
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.
Inadecuada gestión del conflicto de intereses	Un conflicto de intereses surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. Si bien la sola existencia del conflicto de intereses no implica una conducta reprochable, sí existen una serie de comportamientos definidos por códigos de conducta sobre la declaración y gestión del conflicto de intereses. La legislación nacional estima que quien tenga un interés particular en un asunto público está impedido para tomar la decisión.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP contempla que la entidad adopte una serie de instrumentos de gestión del riesgo, que actúe con diligencia en el conocimiento de sus contrapartes y que integre en su operación una función de cumplimiento, todo esto además de la identificación y valoración de los riesgos según la metodología definida en la Política para la Gestión Integral de Riesgos que adopte.

10.2 CONTEXTO DE LA ORGANIZACIÓN

Además, del contexto interno y externo que se realiza, 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.
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. Identificar los lugares en qué opera por su misión, como otras jurisdicciones, sectores, industrias o mercados específicos.
d. La naturaleza, escala y complejidad de los procesos, servicios, trámites u otras operaciones administrativas de la organización, 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 que permita a conocer (naturaleza jurídica, modalidad de selección más recurrente, valores mínimos, máximos y media de contratación, relación de cumplimiento o incumplimientos, tipos de supervisión)
f. Las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización.
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).
h. Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales.

10.3 OPERATIVIDAD DE LOS RIESGOS PARA LA INTEGRIDAD PÚBLICA

Los riesgos para la integridad pública deben ser gestionados en conjunto con los riesgos generales de gestión, la gestión preventiva del riesgo fiscal y los riesgos de seguridad de la información. En consecuencia, se aplicará la misma metodología, y en este aparte de la guía se hará referencia únicamente a particularidades que pueden contribuir a dar mayor claridad o especificidad, así:

10.4 PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

10.4.1 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO LA/FT/FP

En el marco de la gestión del riesgo de LA/FT/FP, debe tenerse en cuenta actividades dentro del flujo de los procesos que implican un intercambio de recursos, bien sea porque la entidad recibe un bien o servicio por el cual paga un precio, o porque entrega un bien o servicio por el cual le pagan un precio. Estas operaciones son los puntos de riesgo relevantes.

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

10.4.2 IDENTIFICACIÓN DE ÁREAS DE IMPACTO LA/FT/FP

Además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

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

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

Las consecuencias legales y de contagio, para efectos de determinar el impacto del riesgo, deben analizarse en términos de **afectación económica**. Se puede estimar que un riesgo se ha materializado cuando la situación que se había identificado como posible (riesgo) ocurre realmente y genera un impacto negativo sobre los objetivos.

La **consecuencia reputacional**, por ejemplo, surge cuando la organización se ve involucrada en denuncias o reportajes que la vinculan con prácticas poco íntegras, incumplimientos normativos o corrupción en general.

La **consecuencia económica** puede configurarse, incluso, desde el mismo momento en que hay retrasos en la ejecución del recurso, por conductas poco íntegras del ejecutor.

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

10.4.3 IDENTIFICACIÓN DE FACTORES DE RIESGO

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

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

10.4.4 DESCRIPCIÓN DEL RIESGO

Teniendo en cuenta las amenazas descritas anteriormente, 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, se podrán tener en cuenta los siguientes ejemplos:

Tabla 17. *Ejemplos descripción del riesgo LA/FT/FP*

Impacto	Causa Inmediata		Causa Raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]".	
	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]".	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

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

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

- Posibilidad de afectación económica por Corrupción en la evaluación en la evaluación de los procesos de selección para la contratación de bienes y servicios de la Entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico.
- Posibilidad de afectación económica por Fraude Interno en la asignación de subsidios a causa de errores, omisiones, informes inexactos o descripciones incorrectas realizados para beneficio personal o de terceros en la asignación de subsidios
- Posibilidad de afectación reputacional por Soborno Saliente en el seguimiento a la agenda legislativa de la Entidad, a causa del ofrecimiento indebido de incentivos o recompensas para que una persona actúe o se abstenga de actuar en favor de la entidad.
- Posibilidad de afectación reputacional por Soborno Entrante al aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.
- Posibilidad de afectación económica por conflicto de interés no declarado y/o declarado, pero no gestionado y/o declarado y no aceptado, a causa de decisiones en asuntos sobre los cuales la servidora o servidor público tiene un interés particular en desarrollo del comité de contratación.

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

Tabla 18. *Análisis riesgos LA/FT/FP*

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

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

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

10.5 PASO 2: 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 la metodología transversal. Así mismo, aplica la matriz de severidad definida en la Guía para la Gestión Integral del Riesgo versión 7 del DAFP, la cual no es susceptible de ajustes.

10.6 PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES

Se tendrá en consideración lo establecido en el Manual para el desarrollo del principio de debida diligencia, el cual incluye una lista de controles generales a nivel entidad y por proceso, los cuales se pueden aplicar en cada uno de los riesgos identificados, sin perjuicio de que puedan desarrollarse controles adicionales o específicos. y/o formular una serie de herramientas de gestión.

10.7 PASO 4: VALORACIÓN DE RIESGO RESIDUAL

No hay nada específico frente a la metodología para la gestión integral del riesgo

SOMOSIG Sistema Integrado de Gestión

CAPÍTULO IV RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad y privacidad de la información se fundamenta en un proceso sistemático de identificación, análisis y valoración de riesgos, orientado a prevenir o minimizar efectos adversos, fortalecer la mejora continua y determinar tanto las consecuencias potenciales como la probabilidad de ocurrencia. En este contexto, la implementación de controles se alinea con lo establecido en el Anexo A de la norma ISO/IEC 27001:2022, considerando la afectación sobre los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad, aplicados a los activos o grupos de activos dentro de cada proceso.

Bajo este enfoque, la gestión de riesgos asociados a los activos de información parte de la identificación de vulnerabilidades y amenazas, así como del análisis de sus posibles impactos. Este ejercicio permite definir, implementar y hacer seguimiento a los controles pertinentes, con el propósito de mitigar la materialización de riesgos y reducir sus efectos sobre la operación y los objetivos institucionales.

10.8 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

La identificación de activos de información se realiza de manera estructurada conforme a los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la Guía de Administración del Riesgo versión 7.0, partiendo del reconocimiento de los procesos institucionales y la determinación de los recursos de información que soportan el cumplimiento de sus objetivos. Este ejercicio contempla la clasificación y caracterización de los activos, incluyendo información, software, hardware, servicios, talento humano y recursos tecnológicos, así como la definición de sus responsables, ubicación, criticidad y relación con los procesos. De esta forma, se establece una base integral que permite analizar su valor para la entidad y su nivel de exposición frente a riesgos, facilitando la posterior evaluación y tratamiento de amenazas y vulnerabilidades en el marco de la gestión integral del riesgo.

El instrumento de levantamiento de activos de información F-E-GET-18 del Ministerio está construido con base en la siguiente estructura:

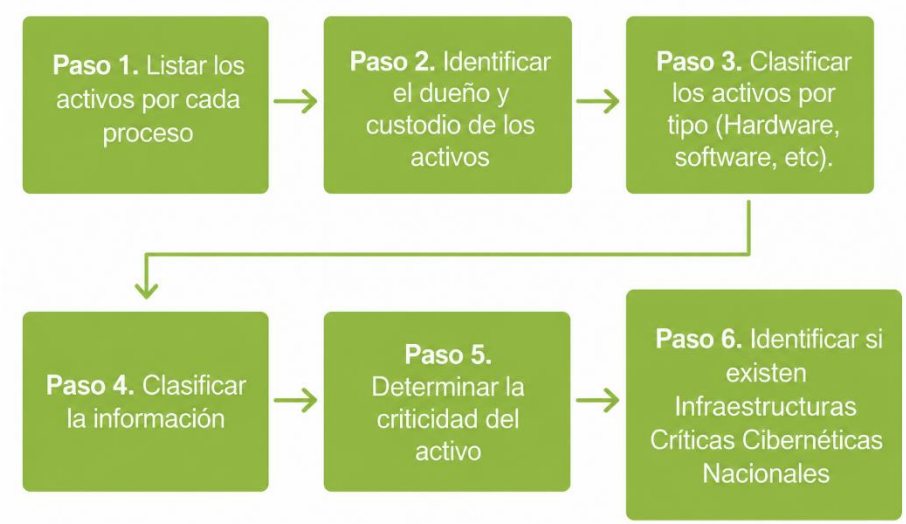

Imagen 20. *Pasos levantamiento activos de información*
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

El proceso de identificación, valoración y clasificación de los activos de información se hace conforme a lo establecido en el I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información

10.9 PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

A partir del inventario actualizado de activos de información de cada proceso, consolidado en el formato F-E-GET-18 "Matriz de Inventario de Activos de Información – Ministerio de Ambiente y Desarrollo Sostenible", se realiza el análisis para identificar los riesgos de seguridad y privacidad de la información. Este análisis contempla la evaluación de amenazas, vulnerabilidades y el impacto potencial que podrían generar sobre los activos identificados. Como resultado, se documentan los riesgos de seguridad de la información asociados a aquellos activos que hayan sido clasificados como críticos.

La evaluación de estos riesgos inicia con la identificación y selección del proceso a analizar en el formato F-E-SIG-28 "Mapa de Riesgos Institucional", para este ejercicio, es fundamental contar con la información base del proceso, incluyendo su objetivo, alcance, inventario de activos de información y demás documentación relevante, con el fin de garantizar una adecuada gestión, evaluación y tratamiento de los riesgos identificados.

La clasificación de los activos identificados se realiza conforme a las siguientes categorías:

Tabla 19. *Clasificación de los activos de información*

Tipo de Activo	Definición	Ejemplos
Información	Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros	- Personales: Bases y archivo de datos, hojas de vida - Financieros: Balances financieros, etc. - Legales: Acuerdos de confidencialidad, entre otros. - Investigación y desarrollo: Licencias, estudios, etc. - Estratégicos: Planes, indicadores, seguimientos, etc. - Otros: Documentación de sistemas de información, copias de seguridad etc.
Software	Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas	- Sistemas operativos - Herramientas Ofimáticas - Motor de bases de datos - Antivirus - Software Estadístico - Software de Georreferenciación - Motores de bases de datos - Software de diseño y programación - Compiladores
Hardware	Corresponden al tipo de activo utilizados para realizar la captura, procesamiento, almacenamiento difusión y divulgación de la información. Se refiere a todos los elementos físicos que permiten el funcionamiento de un medio informático.	- Discos duros o extraíbles - Servidores físicos o virtuales - Computadores - Dispositivos móviles
Servicios	Se relaciona con los servicios tecnológicos proporcionados por la entidad para el apoyo de las actividades de los procesos, las cuales facilitan la administración o el flujo de información.	- Internet - Correo electrónico - Comunicaciones - Directorios compartidos - Aplicaciones - Servicio de correspondencia
Infraestructura física	Recursos requeridos por la entidad para la operación eficaz de los procesos. Corresponden a lugares donde se almacenan o resguardan los sistemas de información y comunicaciones, archivo documental. Espacio o área asignada para alojar y salvaguardar los datos o información considerados como activos críticos para la entidad.	- Edificaciones - Centros de computo - Archivo Central
Recurso Humano	Se refiere a aquellas personas (funcionarios y contratistas) que, por su	- Administradores de infraestructura - Expertos técnicos

Tipo de Activo	Definición	Ejemplos
	conocimiento, experiencia, información histórica y criticidad para el proceso, son consideradas activos de información.	- funcionarios con memoria institucional - Administradores de seguridad - Proveedores - Consultores
Bases de datos personales	Conjunto de datos y registros que caracterizan a personas naturales o jurídicas	- Base de datos de historias laborales - Base de datos de identificación personal - Base de datos de procedimientos administrativos - Base de datos de salud - Bases de datos de contactos con otras entidades - Bases de datos a inscripción de cursos ofertados por el Ministerio
Infraestructura crítica cibernética	Es la infraestructura soportada por las tecnologías de la Información y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el estado.	- Página Web -Aplicativos de trámites y servicios - Otros

10.9.1 TIPO DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

El tipo de riesgo de seguridad de la información se determina con base en la posible afectación a los principios fundamentales de confidencialidad, integridad y disponibilidad de los activos de información. En este sentido, se clasifica el riesgo según la pérdida de confidencialidad cuando la información es accedida o divulgada sin autorización; pérdida de integridad cuando se presenta alteración, modificación o corrupción de los datos; y pérdida de disponibilidad cuando la información o los servicios asociados no se encuentran accesibles en el momento requerido. Esta categorización permite orientar el análisis del impacto y la definición de controles adecuados para la protección de los activos de información.

La clasificación establecida en los tipos de riesgo digital se enfoca de acuerdo con los tres pilares de la seguridad como lo son:

Tabla 20. *Clasificación tipos de riesgo digital*

Tipo de riesgo digital	Descripción
Posibilidad de Pérdida de Confidencialidad	Riesgo de que información sensible o recursos privilegiados sean accedidos por personas no autorizadas, comprometiendo la privacidad y el secreto institucional.
Posibilidad de Pérdida de Disponibilidad	Riesgo de que la información o los recursos no estén accesibles o utilizables cuando se requieran, en el lugar, formato o momento adecuado, afectando la continuidad operativa.
Posibilidad de Pérdida de Integridad	Riesgo de que la información sea modificada, alterada o eliminada total o parcialmente sin autorización, afectando su exactitud, confiabilidad y trazabilidad.

10.9.2 TIPO DE RIESGOS FRENTE A LOS DATOS PERSONALES

Los riesgos asociados al tratamiento de datos personales se clasifican considerando impactos específicos sobre los derechos y libertades de los titulares, tales como la pérdida de confidencialidad, el acceso no autorizado, el uso indebido, la alteración de la información o la indisponibilidad de los datos. No obstante, estos riesgos incorporan consideraciones adicionales frente a los de seguridad de la información, en atención a su naturaleza jurídica y regulatoria, incluyendo el cumplimiento de los principios establecidos en la normativa de protección de datos, la finalidad del tratamiento, la calidad y veracidad de la información, así como las obligaciones del responsable y del encargado. En este sentido, su gestión debe contemplar un enfoque integral que articule aspectos técnicos, legales y organizacionales para garantizar la adecuada protección de los datos personales.

Tabla 21. *Tipos de riesgo de bases de datos personales*

Tipo de riesgo de bases de datos personales	Descripción
Posibilidad de afectación de la disponibilidad de la plataforma tecnológica, herramientas o aplicativos que gestionan datos personales	Ausencia de medidas que permitan garantizar el acceso oportuno y uso de los datos personales por parte de las personas interesadas.
Posibilidad de pérdida de confidencialidad, divulgación no autorizada o uso inadecuado de la información de datos personales	Los datos personales son divulgados y expuestos a terceros. Son usados para otras finalidades distintas a los cuales fueron autorizadas por el propietario de estos. Se realiza un manejo inadecuado de los datos personales.
Posibilidad de pérdida de integridad, alteración, o modificación de la información de datos personales	Carencia de exactitud de los datos personales debido a la manipulación o modificación de estos ya sea de forma accidental o malintencionada.
Posibilidad de sanciones, quejas, reclamos, solicitudes por incumplimiento de las directrices o normativas frente al tratamiento de los datos personales.	Aplicación de posibles medidas por incumplimiento a la normatividad prevista en la ley 1581 de 2012 y demás que la actualizan y la reglamentan, relacionada con la violación de la confidencialidad, disponibilidad o integridad de los datos personales.

10.9.3 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Para una adecuada gestión del riesgo de seguridad de la información es necesario comprender y aplicar los siguientes conceptos clave de acuerdo con la ISO/IEC 27001:2022

Amenaza: Causa potencial de un incidente no deseado, que puede explotar una vulnerabilidad y generar un impacto negativo sobre un activo de información, Las amenazas pueden ser de origen interno o externo,

intencionales o accidentales, y pueden estar relacionadas con factores humanos, tecnológicos, físicos o ambientales.

Vulnerabilidad: Es una debilidad o condición susceptible de ser explotada en un activo de información, en los controles existentes o en un proceso, que puede ser aprovechada por una amenaza para causar un incidente de seguridad de la información.

Para cada riesgo identificado, se deben analizar las amenazas y vulnerabilidades que podrían causar su materialización, con el fin de comprender el origen del riesgo y definir los controles de seguridad adecuados.

Es importante precisar que la sola presencia de una vulnerabilidad no genera daño por sí misma; para que una vulnerabilidad produzca impacto, es necesario que exista una amenaza asociada que pueda explotarla. En consecuencia, una vulnerabilidad que no se encuentre vinculada a una amenaza identificada podría no requerir la implementación de un control.

Para la identificación de las amenazas y vulnerabilidades a las que está expuesto cada activo de información, se puede utilizar como referencia la Tabla 22 el cual incluye la tabla de amenazas comunes y la Tabla 23 que relaciona las vulnerabilidades comunes, diseñadas como herramientas de apoyo para las áreas en el análisis y gestión de riesgos de seguridad de la información.

Tabla 22. *Amenazas comunes*

Tipo	Descripción de Amenaza
Amenazas Físicas	Contaminación, Polvo, Corrosión.
	Niveles de temperatura o humedad por fuera de los rangos aceptables.
	Incendio.
	Daño en instalaciones físicas.
	Desastres naturales.
	Asonada/Conmoción civil / Terrorismo/Vandalismo.
	Desastre accidental.
	Contaminación, radiación nociva
	Agua
	Explosión
Amenazas Naturales	Fenómeno Sísmico
	Fenómeno meteorológico
	Inundación.
	Fenómeno pandémico/epidémico
	Fenómeno volcánico
Acciones Humanas	Sobrecarga laboral.
	Ingeniería social.
	Hurto de medios o documentos
	Espionaje remoto
	Hurto de equipos

Tipo	Descripción de Amenaza
	Hurto de identidad o credenciales digitales
	Recuperación de soportes reciclados o desechados.
	Divulgación de la información
	Sabotaje.
	Exploits usando comunicación basada en la web
	Introducción de datos de fuentes no confiables
	Manipulación del hardware
	Manipulación con software
	Acciones fraudulentas
	Tratamiento no autorizado de datos personales
	Entrada no autorizada a las instalaciones
	Uso no autorizado de dispositivos
	Incumplimiento en la disponibilidad del personal
	Uso incorrecto de los dispositivos
	Deterioro de dispositivos o soportes
	Entrega indebida de la información.
	Copia fraudulenta de software
	Uso de software falsificado o copiado
	Tratamiento ilegal de datos
	Envío o distribución de malware
	Corrupción de datos
	Atentado terrorista
	Interceptación de la radiación de un dispositivo
	Escucha clandestina
	Ataque de descarga oculta a través de internet
	Ataque de repetición, ataque de intermediario
	Detección de posición
Fallas en la Infraestructura	Fallas de electricidad.
	Fallo de red de telecomunicaciones
	Fallo del equipo de telecomunicaciones
	Fallas en el aire acondicionado.
	Fallas en las UPS.
	Fallas en la planta eléctrica.
	Señales de interferencia.
	Radiación electromagnética
	Daño en componentes tecnológicos
	Fallas en un sistema de suministro
	Radiación térmica
	Impulsos electromagnéticos

Tipo	Descripción de Amenaza
Fallas técnicas	Falla del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Compromiso de las funciones	Error de uso
	Abuso de derechos o permisos
	Interceptación de señales de interferencia comprometedoras
	Falsificación de derechos o permisos
	Denegación de acciones
Amenazas para la organización	Falta de personal
	Falta de recursos
	Fallo de los proveedores de servicios
	Violación de leyes o reglamentos

Fuente: Adaptada Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas 2025 y ajustado por la OTIC

Tabla 23. *Vulnerabilidades comunes*

Tipo	Descripción de Vulnerabilidad
Hardware	Mantenimiento insuficiente o inoportuno de los componentes de hardware.
	Falta de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Falta de control de cambio con configuración eficiente
	Susceptibilidad a las variaciones de tensión.
	Dependencia de un sólo proveedor de Internet.
	Susceptibilidad a las variaciones de temperatura.
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Obsolescencia tecnológica.
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Defectos conocidos en el software
	Ausencia de "cierre de sesión" al abandonar el puesto de trabajo
	Eliminación o reutilización de los medios de almacenamiento sin un borrado adecuado
	Configuración insuficiente de los registros con fines de auditoría
	Asignación incorrecta de los derechos de acceso
	Software ampliamente distribuido
	Aplicación de programas de aplicación a los datos erróneos en términos de tiempo

Tipo	Descripción de Vulnerabilidad
	Interfaz de usuario complicada
	Insuficiente o falta de documentación
	Configuración incorrecta de los parámetros
	Mecanismos de identificación y autenticación insuficientes
	Tablas de contraseñas desprotegidas
	Mala Gestión de las contraseñas
	Servicios innecesarios habilitados
	Software inmaduro o nuevo
	Especificaciones poco claras o incompletas para los desarrolladores
	Control de cambios ineficaz
	Descarga y uso incontrolado de software
	Falta de copias de seguridad o copias incompletas
	Falta de elaboración de informes de gestión
	Fechas incorrectas
Red	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje
	Líneas de comunicación desprotegidas
	Tráfico sensible desprotegido
	Cableado conjunto deficiente
	Punto único de falla
	Ineficacia o falta de mecanismos de identificación y autenticación del emisor y el receptor
	Arquitectura de red insegura.
	Transferencia de contraseñas autorizadas
	Gestión inadecuada a la red (resiliencia del enrutamiento)
	Conexiones de red pública no protegidas
Personal	Ausencia de personal
	Procedimientos de contratación inadecuados
	Formación insuficiente en materia de seguridad
	Uso incorrecto del software y hardware
	Escasa concienciación en materia de seguridad
	Falta de mecanismos de monitoreo
	Trabajo no supervisado por personal externo o de limpieza
	Ineficacia o falta de políticas para el uso correcto de los medios de telecomunicación y mensajería.
	Desconocimiento del marco legal y regulatorio de seguridad de la información.
	Desconocimiento de los controles de seguridad informática aplicados a los activos de información que son de su responsabilidad.
	Desconocimiento del marco legal y regulatorio de la protección de los datos personales.
	Desconocimiento de políticas, normas, o procedimientos para el tratamiento de los datos personales.

Tipo	Descripción de Vulnerabilidad
Sitio	Uso inadecuado o descuidado del control de acceso físico a edificios y salas
	Ubicación en una zona susceptible de inundación
	Insuficiente protección física del edificio, puertas y ventanas
	Red eléctrica inestable
Organización	No se ha desarrollado un procedimiento formal para el registro y la cancelación de usuarios, o su aplicación es ineficaz
	No se ha desarrollado un procedimiento formal para la revisión de los derechos de acceso (supervisión), o su aplicación es ineficaz.
	Disposiciones insuficientes (relativas a la seguridad) en los contratos con clientes y/o terceros.
	No se ha desarrollado un procedimiento de supervisión de las instalaciones de procesamiento de la información, o su aplicación es ineficaz.
	No se realizan auditorías (supervisión) de forma regular
	No se han desarrollado procedimientos de identificación y evaluación de riesgos, o su aplicación es ineficaz
	Insuficiencia o falta de informes de fallos registrados en los registros de los administradores y operadores
	Respuesta inadecuada del servicio de mantenimiento
	Acuerdo de nivel de servicio insuficiente o inexistente.
	No se ha desarrollado un procedimiento de control de cambios, o su aplicación es ineficaz.
	No se ha desarrollado un procedimiento formal para el control de la documentación del SGSI, o su aplicación es ineficaz.
	No se ha desarrollado un proceso formal para la autorización de la información disponible al público, o su implementación es ineficaz.
	Asignación inadecuada de las responsabilidades de seguridad de la información.
	No existen planes de continuidad, o son incompletos, o están obsoletos
	No se ha desarrollado una política de uso del correo electrónico o su aplicación es ineficaz.
	No se han elaborado procedimientos para la introducción de programas informáticos en los sistemas operativos, o su aplicación es ineficaz.
	No se han desarrollado procedimientos para la introducción de programas informáticos en los sistemas operativos, o su aplicación es ineficaz.
	No se han desarrollado procedimientos para el manejo de información clasificada, o su aplicación es ineficaz.
	Las responsabilidades de seguridad de la información no están presentes en las descripciones de los puestos de trabajo.

Tipo	Descripción de Vulnerabilidad
	Insuficiencia o falta de disposiciones (relativas a la seguridad de la información) en los contratos de los empleados.
	El proceso disciplinario en caso de incidente de seguridad de la información no está definido, o no funciona correctamente
	No se ha desarrollado una política formal sobre el uso de ordenadores móviles, o su aplicación es ineficaz
	Insuficiente control de los activos fuera de las instalaciones
	Insuficiente o falta de política de "escritorio y pantalla limpios".
	Autorización de las instalaciones de procesamiento de la información no implementada o que no funciona correctamente
	Mecanismos de supervisión de las violaciones de la seguridad no aplicados adecuadamente
	Procedimientos de notificación de deficiencias de seguridad no desarrollados, o su aplicación es ineficaz
	No se han desarrollado procedimientos de cumplimiento de las disposiciones en materia de derechos intelectuales, o su aplicación es ineficaz
	Proceso disciplinario en incidentes no definido
	SLA inexistente o insuficiente
	Procedimientos sobre derechos de propiedad intelectual inexistentes

Fuente: Adaptada Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas 2025 y ajustado por la OTIC

SOMOSIG Sistema Integrado de Gestión

10.9.4 IDENTIFICACIÓN DE CONSECUENCIAS

Las consecuencias corresponden al impacto que la materialización de un riesgo de seguridad de la información puede generar en la entidad y en sus procesos. Dichas consecuencias, pueden ser: legales, económicas, operativas, sociales y reputacionales y deben ser consideradas durante el análisis del riesgo.

A continuación, se listan las consecuencias identificadas para la evaluación de los riesgos de seguridad de la información:

Tabla 24. *Consecuencias riesgos seguridad de la información*

Consecuencias
Acceso de la información por parte de personal no autorizado
Accesos no autorizados en instalaciones físicas (Centro de cómputo, cableado, edificios, entre otros)
Daños de imagen, reputación y buen nombre del proceso o institucional
Demoras en la prestación de los servicios de información, misionales o tecnológicos
Demoras en los procesos administrativos institucionales para el desarrollo de su gestión
Falla (s) en el funcionamiento de los sistemas de información
Incumplimiento Ley de protección de datos personales y Hábeas Data.
Incumplimientos legales o normativos

Consecuencias
Indisponibilidad de la información institucional a los usuarios
Investigaciones, hallazgos y posibles sanciones de los Entes de control internos y externos
Pérdida o eliminación de la información
Pérdida parcial o total de información física o digital
Pérdidas económicas
Publicación de datos personales o confidenciales
Quejas y reclamos de los usuarios
Reprocesos administrativos o financieros para intentar restaurar la información
Reprocesos, demoras y paralizaciones en la ejecución de actividades
Robo de datos y equipos
Suplantación de la identidad
Toma de decisiones inadecuadas

Fuente: Adaptado de Guía de Gestión de Riesgos – MINTIC

10.10 PASO 2: ANÁLISIS DE RIESGO INHERENTE

Para el cálculo de probabilidad e impacto, aplica la metodología transversal. Así mismo, aplica la matriz de severidad definida en la Guía para la Gestión Integral del Riesgo versión 7 del DAFP.

10.11 PASO 3: IDENTIFICACIÓN DE CONTROLES

Una vez realizado el análisis del riesgo inherente, se deben identificar y determinar los controles que permitirán tratar los riesgos identificados.

La identificación de controles se realiza de manera conjunta entre el enlace de seguridad de la información y el equipo de trabajo del proceso, quienes, con base en el conocimiento del activo de información, del proceso y del contexto operativo, determinan los controles existentes y los controles adicionales que se requieran implementar para la mitigación del riesgo.

La entidad adopta como referencia mínima los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2022, aunque se pueden definir controles adicionales de acuerdo con las necesidades de la entidad. Como apoyo para la identificación y selección de dichos controles, estos se encuentran relacionados y consolidados en la tabla 27.

La descripción del control debe definir el responsable, la acción de control e incluir los atributos de formalización: documentación soporte, frecuencia, evidencia generada y forma de ejecución.

A continuación, se presenta un ejemplo de identificación y descripción de un control de seguridad de la información, en el cual se realiza una descripción de la forma en la cual el control seleccionado será o está implementado en la entidad.

Tabla 25. *Ejemplo identificación de controles seguridad de la información*

Nombre del Control	Descripción del Control
6.3 Conciencia de Seguridad de la Información, educación y formación	El Líder de capacitaciones del proceso de talento humano ejecuta las actividades del Plan Institucional de Capacitación (PIC) dejando registro de participación de los procesos y el El Oficial de seguridad de la Información verifica y realiza seguimiento al cronograma de sensibilizaciones de Seguridad de la información.

10.11.1 DOMINIO

Para los riesgos de Seguridad de la Información los dominios en la ISO 27001 corresponden a categorías o áreas temáticas principales de la seguridad de la información. Cada dominio agrupa objetivos de control y controles relacionados, proporcionando una estructura organizativa para los requisitos de seguridad. En este apartado, la información se encuentra organizada con respecto a los 14 dominios definidos en la ISO 27001, abarcando así de manera integral los aspectos clave de la gestión de la seguridad de la información, así:

Tabla 26. *Lista de dominios anexo A*

Dominio
A.5 Organizacional
A.6 Controles de Personas
A.7 Controles físicos
A.8 Controles Tecnológicos

Fuente: ISO 27001:2022

SOMOSIG Sistema Integrado de Gestión

10.11.2 CONTROLES ISO 27001

Para los riesgos de Seguridad de la Información los controles relacionados en este apartado se encuentran alineados con los 93 controles del anexo A de la ISO 27001 y deben considerarse para mitigar las causas que hacen que el riesgo se pueda materializar conforme a las vulnerabilidades identificadas.

Los controles relacionados en este apartado se encuentran alineados con los 93 controles del anexo A de la ISO 27001 y deben considerarse para mitigar las causas que hacen que el riesgo se pueda materializar conforme a las vulnerabilidades identificadas, como se describe a continuación:

Tabla 27. *Controles Anexo A ISO27001:2022*

Claúsula o Dominio	Nombre del Control
Controles Organizacionales	5.1. Políticas de seguridad de la información
	5.2. Roles y responsabilidades en la seguridad de la información
	5.3. Segregación de deberes
	5.4. Responsabilidades de la dirección
	5.5. Contacto con las Autoridades
	5.6. Contacto con grupos de interés especial
	5.7. Inteligencia de amenazas

Claúsula o Dominio	Nombre del Control
	5.8. Seguridad de la información en la gestión de proyectos
	5.9. Inventario de información y otros activos asociados
	5.10. Uso aceptable de la información y otros activos asociados
	5.11. Devolución de los activos
	5.12. Clasificación de la información
	5.13. Etiquetado de la información
	5.14. Transferencia de información
	5.15. Control de acceso
	5.16. Gestión de identidades
	5.17. Información de autenticación
	5.18. Derechos de acceso
	5.19. Seguridad de la información en relaciones con proveedores
	5.20. Abordar la seguridad de la información dentro de los acuerdos con los proveedores
	5.21. Gestión de la seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)
	5.22. Seguimiento, revisión y gestión del cambio de los servicios de los proveedores
	5.23. Seguridad de la información para el uso de servicios en la nube
	5.24. Planificación y preparación de la gestión de incidentes de seguridad de la información
	5.25. Evaluación y decisión sobre eventos de seguridad de la información
	5.26. Respuesta a incidentes de seguridad de la información
	5.27. Aprender de los incidentes de seguridad de la información
	5.28. Recopilación de evidencias
	5.29. Seguridad de la información durante una interrupción
	5.30. Preparación de las TIC para la continuidad del negocio
	5.31. Requisitos legales, reglamentarios y contractuales
	5.32. Derechos de propiedad intelectual
	5.33. Protección de registros
	5.34. Privacidad y protección de la información de identificación personal (PII, por sus siglas en ingles)
	5.35. Revisión independiente de la seguridad de la información
	5.36. Cumplimiento de políticas, reglas y estándares de seguridad de la información
	5.37. Procedimientos operativos documentados
Controles de Personas	6.1. Selección
	6.2. Términos y condiciones de empleo
	6.3. Conciencia de seguridad de la información, educación y formación
	6.4. Proceso disciplinario
	6.5. Responsabilidades después de la terminación o cambio de empleo
	6.6. Acuerdos de confidencialidad o no divulgación
	6.7. Trabajo remoto

Claúsula o Dominio	Nombre del Control
	6.8. Informes de eventos de seguridad de la información
Controles Físicos	7.1. Perímetros de seguridad física
	7.2. Entrada física
	7.3. Asegurar oficinas, habitaciones e instalaciones
	7.4. Monitoreo de la seguridad física
	7.5. Protección contra amenazas físicas y ambientales
	7.6. Trabajar en áreas seguras
	7.7. Escritorio y pantalla limpios
	7.8. Emplazamiento y protección de equipos
	7.9. Seguridad de los activos fuera de las instalaciones
	7.10. Medios de almacenamiento
	7.11. Servicios públicos de apoyo
	7.12. Seguridad del cableado
	7.13. Mantenimiento de equipos
	7.14. Disposición o reutilización segura de los equipos
Controles Tecnológicos	8.1. Dispositivos de punto final de usuario
	8.2. Derechos de acceso privilegiado
	8.3. Restricción de acceso a la información
	8.4. Acceso al código fuente
	8.5. Autenticación segura
	8.6. Gestión de la capacidad
	8.7. Protección contra malware
	8.8. Gestión de vulnerabilidades técnicas
	8.9. Gestión de la configuración
	8.10. Eliminación de información
	8.11. Enmascaramiento de datos
	8.12. Prevención de fugas de datos
	8.13. Copia de seguridad de la información
	8.14. Redundancia de las instalaciones de procesamiento de información
	8.15. Registro
	8.16. Actividades de seguimiento
	8.17. Sincronización de reloj
	8.18. Uso de programas de utilidad privilegiados
	8.19. Instalación de software en sistemas operativos
	8.20. Seguridad de redes
	8.21. Seguridad de los servicios de red
	8.22. Segregación de redes
	8.23. Filtrado web
	8.24. Uso de la criptografía
	8.25. Ciclo de vida de desarrollo seguro
	8.26. Requisitos de seguridad de las aplicaciones

Claúsula o Dominio	Nombre del Control
	8.27. Arquitectura de sistemas seguros y principios de ingeniería
	8.28. Codificación segura
	8.29. Pruebas de seguridad en el desarrollo y aceptación
	8.30. Desarrollo externalizado
	8.31. Separación de entornos de desarrollo, evidencia y producción
	8.32. Gestión del cambio
	8.33. Información de las pruebas
	8.34. Protección de los sistemas de información durante las pruebas de auditoria

10.12 PASO 4: VALORACIÓN DE RIESGO RESIDUAL

No hay nada específico frente a la metodología para la gestión integral del riesgo

10.13 REVISIÓN Y MONITOREO

La Oficina de Tecnologías de la Información y la Comunicación realizará seguimiento y monitoreo a los planes de tratamiento una vez al año para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad de la información para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

CAPÍTULO V RIESGOS AMBIENTALES

La presente Guía se aplicará de manera integral a la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos y oportunidades asociados al Sistema de Gestión Ambiental – SGA del Ministerio de Ambiente y Desarrollo Sostenible. Para tal efecto, los riesgos ambientales se entenderán como aquellos eventos potenciales que puedan afectar el cumplimiento de los objetivos ambientales institucionales, el desempeño ambiental del Ministerio y el acatamiento de las obligaciones de cumplimiento ambientales, considerando los aspectos ambientales significativos y los asuntos relevantes del contexto interno y externo, incluidos el cambio climático, la economía circular y la protección de la biodiversidad.

El levantamiento y administración de los riesgos del SGA se realizará utilizando las etapas, criterios, escalas y matrices establecidos en el Capítulo I de esta Guía, registrándolos en las matrices institucionales de riesgos y en el mapa de riesgos integral, asegurando que los riesgos ambientales identificados cuenten con controles y planes de tratamiento articulados con los controles operacionales, los objetivos, las metas, los indicadores y los programas ambientales del Ministerio, así como con los mecanismos de seguimiento y mejora continua definidos para el SIG.

10.14 PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO AMBIENTAL

Se realiza a partir de:

- Los objetivos ambientales, la identificación de procesos con aspectos ambientales significativos, programas e indicadores establecidos en el SGA.
- Las obligaciones de cumplimiento ambientales (requisitos legales y otros requisitos) aplicables al Ministerio.
- La materialización afecte directamente el logro de esos objetivos (energía, agua, residuos, huella de carbono, compras sostenibles, emergencias ambientales).
- Los asuntos del contexto interno, externo y demás relacionados con cambio climático, economía circular - cadena de suministros, biodiversidad y degradación ambiental.

Los puntos de riesgo, áreas de impacto, factores de riesgo y descripción de riesgos se definirán, asegurando que los eventos potenciales identificados afecten o puedan afectar el desempeño ambiental institucional teniendo presente que:

- Puntos de riesgo ambientales: Usar la caracterización de procesos, el contexto estratégico y los controles operacionales ambientales para localizar actividades donde puedan ocurrir eventos de riesgo ambiental (consumo de recursos, generación y manejo de residuos, almacenamiento de sustancias, mantenimiento, servicios tercerizados, viajes/actividades en territorio, etc.).

  Incluir puntos de riesgo “aguas arriba y aguas abajo” relacionados con proveedores/contratistas y con la implementación de políticas e instrumentos normativos que puedan derivar en emergencias o impactos relevantes.

- Áreas de impacto para riesgos ambientales: Considerar el impacto ambiental (afectación al entorno, recursos naturales, clima, biodiversidad) y su traducción en impacto reputacional e incluso económico para la entidad, usando los criterios de impacto de la Guía.

  Cuando aplique, vincular el impacto con compromisos externos (ODS, metas nacionales de clima y biodiversidad, política ambiental).

10.15 PASO 2. ANÁLISIS DE RIESGO INHERENTE RIESGO AMBIENTAL

Cuando se valoren riesgos ambientales del SGA:

- La probabilidad se determinará con base en la frecuencia de las actividades asociadas a los aspectos ambientales significativos (operación normal, anormal y emergencias) y en la exposición a factores de contexto ambiental, incluidos escenarios de cambio climático. (por ejemplo, número de operaciones de mantenimiento, número de eventos, frecuencia de generación de residuos, número de contratos ambientales al año). Una actividad permanente se considerará “muy alta”.

- El impacto considerará de manera integrada:
  - La magnitud del impacto sobre el medio ambiente (recursos naturales, clima, biodiversidad, contaminación).
  - El efecto sobre el cumplimiento de obligaciones de cumplimiento ambientales.
  - Las implicaciones reputacionales (afectación interna, sectorial o nacional) y económicas (Costos de atención de emergencias, sanciones, perdida de recursos) que se deriven de la materialización del riesgo.

La combinación de probabilidad e impacto permitirá ubicar los riesgos ambientales en la matriz de severidad, obteniendo el nivel de riesgo inherente conforme a esta Guía.

10.16 PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES RIESGOS DEL SGA.

Para los riesgos ambientales los controles se identificarán y describirán considerando:

- Los controles operacionales definidos en el SGA (procedimientos, protocolos, programas, residuos, compras sostenibles, emergencias ambientales, entre otros.), asegurando que los mismos atacan la causa raíz relacionada.
- Las acciones planificadas para abordar riesgos y oportunidades ambientales, conforme a ISO 14001.
- Los mecanismos para asegurar el cumplimiento de las obligaciones de cumplimiento ambientales.

10.17 PASO 4: VALORACIÓN DEL RIESGO RESIDUAL.

La valoración de diseño, implementación y eficacia de estos controles seguirá los criterios establecidos en esta Guía, y permitirá determinar el riesgo residual ambiental.

Los riesgos ambientales con nivel residual alto o extremo deberán contar con planes de tratamiento articulados con los programas, objetivos e indicadores del SGA, y su seguimiento será incorporado en:

- El seguimiento a indicadores ambientales.
- La evaluación del cumplimiento de obligaciones de cumplimiento ambientales.
- La revisión por la dirección del Sistema Integrado de Gestión

CAPÍTULO VI RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO

Los riesgos de Seguridad y Salud en el Trabajo corresponden a eventos potenciales derivados de la exposición a peligros físicos, químicos, biológicos, biomecánicos, psicosociales, de condiciones de seguridad y fenómenos naturales, en concordancia con la clasificación utilizada en la GTC 45, presentes en las actividades, procesos, instalaciones y condiciones laborales, que puedan generar afectaciones a la salud accidentes de trabajo, enfermedades laborales, incidentes, emergencias o afectaciones al bienestar de los trabajadores, contratistas, visitantes y demás partes interesadas.

Los riesgos de seguridad y salud en el trabajo específicos deben ser incorporados en el DS-A-ATH 04 Matriz de Identificación de Peligros, Evaluación de Riesgos y Determinación de Controles, conforme a lo establecido en la G-A-ATH-04 “Identificación de Peligros, Evaluación de Riesgos y Establecimiento de Controles – IPEREC”. Esta matriz constituirá el instrumento oficial para la gestión de los riesgos de Seguridad y Salud en el Trabajo de la entidad.

Así mismo, aquellos riesgos que, por su naturaleza o nivel de exposición, puedan afectar el cumplimiento de los objetivos institucionales, la continuidad de la operación, el desempeño organizacional o el cumplimiento de requisitos legales, deberán incorporarse adicionalmente al mapa de riesgos institucional para su seguimiento y tratamiento conforme a lo establecido en el Capítulo I Riesgos Generales de la Gestión.

Las acciones de control y los planes de tratamiento definidos para estos riesgos deberán articularse con el Plan Anual de Trabajo del SG-SST y los demás mecanismos de seguimiento y mejora continua establecidos en el proceso de Administración del Talento Humano.