

MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN

GUÍA PARA LA GESTIÓN DEL RIESGO



Ciencias



TABLA DE CONTENIDO

INTRODUCCIÓN.....4

1 OBJETIVO.....4

2 ALCANCE.....4

3 MARCO NORMATIVO APLICABLE.....4

4 DEFINICIONES.....4

5 PRINCIPIOS QUE SOPORTAN LA GESTIÓN DE RIESGOS.....8

6 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO.....8

6.1 Contenido de la política de administración del riesgo.....8

7 RESPONSABILIDADES LÍNEAS DE DEFENSA EN EL MARCO DE LA GESTIÓN DE RIESGOS.....9

8 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS.....12

9 METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO.....14

9.1 Identificación del Contexto.....15

9.1.1 Análisis de objetivos.....15

9.1.2 Establecimiento del contexto.....16

9.2 Identificación de los puntos de riesgo.....16

9.3 Identificación de áreas de impacto.....16

9.4 Identificación de áreas de factores de riesgo.....16

9.5 Identificación de riesgos.....17

9.5.1 Técnicas para la identificación de riesgos.....17

10 RIESGOS DE GESTIÓN.....17

10.1 Descripción del Riesgo.....17

10.2 Clasificación del Riesgo.....18

10.3 Valoración del Riesgo.....19

10.4 Evaluación del Riesgo.....20

10.5 Valoración de Controles.....21

10.5.1 Estructura para la descripción del control.....21

10.5.2 Tipologías y atributos para el diseño de los controles.....21

10.6 Determinación del riesgo residual.....23

11 RIESGOS DE CORRUPCIÓN O RIESGOS A LA INTEGRIDAD PÚBLICA.....23

11.1 Descripción del Riesgo.....24

11.2 Valoración del Riesgo de Corrupción o riesgo a la integridad pública.....24

11.3 Evaluación del Riesgo de Corrupción o riesgo a la integridad pública.....25

| | | |
|---|--|----------------------------|
|  Ciencias  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 3 de 41 |

| | | |
|----------------|--|-----------|
| 11.4 | Valoración de Controles | 26 |
| 11.5 | Determinación del riesgo residual | 26 |
| 12 | RIESGOS FISCALES | 26 |
| 12.1 | Identificación del Riesgo | 26 |
| 12.2 | Descripción del Riesgo | 26 |
| 12.3 | Valoración del Riesgo Fiscal | 28 |
| 12.4 | Valoración de Controles | 29 |
| 12.5 | Determinación del riesgo residual | 29 |
| 13 | RIESGOS DE SEGURIDAD DE LA INFORMACIÓN | 29 |
| 13.1 | Identificación de los activos de seguridad de la información | 29 |
| 13.2 | Identificación del riesgo de seguridad de la información | 29 |
| 13.3 | Valoración del riesgo de seguridad de la información | 30 |
| 13.4 | Controles asociados a la seguridad de la información | 30 |
| 14 | GESTIÓN DE RIESGOS DE TI | 30 |
| 15 | TRATAMIENTO DEL RIESGO | 31 |
| 15.1 | Plan de manejo de riesgo | 32 |
| 16 | MONITOREO Y SEGUIMIENTO DE RIESGOS | 33 |
| 16.1 | Consideraciones generales para el Monitoreo de Riesgos | 33 |
| 16.2 | Acciones a seguir en caso de Materialización del Riesgo | 33 |
| 16.3 | Periodicidad del monitoreo y seguimiento al mapa de riesgos | 35 |
| 17 | ACTUALIZACIÓN DE LOS MAPAS DE RIESGOS | 36 |
| 18 | COMUNICACIÓN Y CONSULTA | 36 |
| 19 | RIESGOS DE LAVADO DE ACTIVOS Y EL FINANCIAMIENTO DEL TERRORISMO "LA/FT/FPADM" | 37 |
| 20 | GESTIÓN DE LOS RIESGOS DEL SISTEMA DE SEGURIDAD Y SALUD EN EL TRABAJO | 37 |
| 21 | GESTIÓN DE LOS RIESGOS EN LOS PROCESOS DE CONTRATACIÓN | 37 |
| 22 | RIESGOS RELACIONADOS CON CALIDAD ESTADÍSTICA | 38 |
| 23 | RIESGOS EMERGENTES | 38 |
| 24 | BIBLIOGRAFÍA | 38 |
| 25 | DOCUMENTOS ASOCIADOS | 38 |
| 26 | CONTROL DE CAMBIOS | 39 |
| ANEXO 1 | | 40 |

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 4 de 41 |

INTRODUCCIÓN

El Ministerio de Ciencia, Tecnología e Innovación (Ministerio) ejecuta sus actividades bajo un enfoque de gestión por procesos basado en riesgos. El cumplimiento tanto de sus objetivos de proceso como estratégicos puede verse afectado por riesgos tanto positivos como negativos; con la finalidad de mitigarlos o aprovecharlos según el caso, se hace necesario contar con una metodología encaminada a administrar y prevenir su ocurrencia al interior del Ministerio. Dicha metodología contribuye al conocimiento y mejoramiento de la Entidad, a elevar la productividad, a garantizar la eficiencia y eficacia de los procesos organizacionales y permite la definición de estrategias de mejoramiento continuo, brindándole a la Entidad un enfoque en riesgos.

La administración de riesgos se desarrolla a través de la aplicación de esta Guía, la cual toma como referencia los lineamientos del Departamento Administrativo de la Función Pública (DAFP); Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y la Secretaría de Transparencia de la Presidencia de la República en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas"; en concordancia con lo establecido en la Ley 1474 de 2011 y en el Modelo Integrado de Planeación y Gestión, el cual incluye las Líneas de Defensa y define los roles, responsabilidades, actuaciones y políticas a seguir para coadyuvar en la consecución de los objetivos institucionales que se pretenden alcanzar.

La presente guía es un instrumento de tipo preventivo para identificar, analizar, evaluar, tratar, comunicar, monitorear, revisar y realizar seguimiento a los riesgos de gestión, corrupción o riesgos a la integridad pública, fiscales, seguridad de la información y riesgos de tecnologías de la información (TI), con el fin de optimizar y enfocar los esfuerzos institucionales en acciones estandarizadas que permitan abordar y tratar los riesgos identificados en forma eficaz y efectiva para el logro de los objetivos y metas institucionales, potencializando las oportunidades identificadas.

1 OBJETIVO

Definir los lineamientos para la implementación y desarrollo de la política de administración del riesgo y la gestión de las oportunidades del Ministerio, a través de un conjunto de lineamientos orientados a la adecuada gestión de riesgos de proceso, corrupción o riesgos a la integridad pública, fiscales, seguridad de la información y riesgos de TI, identificados en el Sistema Integrado de Gestión (SIG), con el propósito de contar con herramientas para anticiparse a posibles situaciones que afecten el cumplimiento de la misión y objetivos estratégicos del Ministerio.

2 ALCANCE

Esta guía define los lineamientos para la gestión y control de los riesgos de gestión, corrupción o riesgos a la integridad pública, fiscales, seguridad de la información y riesgos de TI, del Ministerio partiendo desde la política de administración del riesgo (numeral 6), la construcción del mapa de riesgos, la comunicación, consulta y divulgación de los riesgos existentes, su priorización, seguimiento, monitoreo, revisión y actualización para la gestión integral de los riesgos.

Se incluyen los lineamientos para la gestión de los riesgos de toda naturaleza, así como las directrices para la gestión de las oportunidades con el fin de garantizar un manejo sistemático, articulado y transversal en todos los procesos y funciones del Ministerio.

3 MARCO NORMATIVO APLICABLE

- 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.
- 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 403 de 2020. Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.
- Directiva Presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.
- Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas - DAFP 2022
- Normograma de la entidad, dispuesto en el sistema de información Gina

4 DEFINICIONES

- Activo: Conjunto de bienes económicos y derechos que posee una entidad. En el contexto de seguridad de la información 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.
- Administración del Riesgo: Comprende el conjunto de elementos de Control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera

D102PR01G01PL03

Versión:01

Fecha: 5/07/2024

negativa el logro de sus objetivos institucionales. La administración del riesgo contribuye a que la entidad consolide su Sistema de Control Interno y a que se genere una cultura de autocontrol y autoevaluación al interior de esta.

- **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.
- **Análisis de Riesgo:** Elemento de control que permite establecer la probabilidad de ocurrencia del riesgo y el impacto o consecuencias, calificándolo y evaluándolo a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos específicos y la magnitud de sus consecuencias.
- **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 (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.
- **Bien de Uso Público:** Aquellos cuyo uso pertenece a todos los habitantes del territorio nacional, por ejemplo: Las calles, plazas, puentes, vías, parques etc.
- **Bienes Fiscales:** Aquellos que están destinados al cumplimiento de las funciones o servicios públicos, es decir, afectos al desarrollo de su misión y utilizados para sus actividades, por ejemplo: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.
- **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.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Ciberseguridad:** Conjunto de medidas de protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.
- **Confidencialidad:** Pilar de seguridad de la información, que consiste en la propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **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.
- **Contraparte:** Hace referencia a cualquier persona natural o jurídica con la que el negocio tenga vínculos comerciales, de negocios, contractuales o jurídicos de cualquier orden. Son contrapartes los accionistas, socios, empleados, clientes y proveedores de bienes y servicios, entre otros. **Financiación del Terrorismo:** Delito que comete toda persona que incurra en alguna de las conductas descritas en el artículo 345 del Código Penal.
- **Control:** Medida o acción para reducir la probabilidad de materialización de un riesgo.
- **Control Manual:** controles que son ejecutados por personas.
- **Control Automático:** son ejecutados por un sistema.
- **Control Correctivo:** Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.
- **Control Detectivo:** Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- **Control Preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- **Control Interno:** Es el proceso que por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, procura que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.
- **Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio privado.
- **Criterio de Frecuencia:** Criterio para medir la probabilidad de ocurrencia, analizando el número de eventos en un periodo determinado, los hechos que se han materializado y el historial de situaciones o eventos asociados al riesgo.
- **Debida diligencia:** Es el proceso mediante el cual las entidades realizan el conocimiento efectivo, eficiente y oportuno de todos los clientes actuales y potenciales. Esto incluye la verificación de la información y los soportes de la misma, es decir de todas personas naturales o jurídicas con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto propio de su actividad.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Evaluación del Riesgo:** Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 6 de 41 |

- **Factor de Riesgo:** Son las fuentes generadoras de riesgos. Es cualquier circunstancia, situación, elemento, proceso, al que se encuentra expuesta la Entidad y que al producirse genera la materialización de un evento.
- **Factores de Riesgo:** Los factores de riesgo, son los agentes generadores del riesgo de LA/FT-FPADM, se deben analizar y segmentar de cara a cada uno de los elementos que lo pueden generar, en especial las contrapartes, los productos, los canales de distribución y las áreas geográficas o jurisdicción.
- **Financiación del terrorismo:** Delito que comete toda persona que incurra en alguna de las conductas descritas en el artículo 345 del Código Penal.
- **Gestión del Riesgo LA/FT-FPADM:** Consiste en la adopción de políticas que permitan prevenir y controlar el riesgo de LA/FT-FPADM.
- **Gestión del Riesgo Fiscal:** Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial), por ejemplo: Los contratistas, los interventores, los supervisores y en general todos los servidores públicos.
- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado, por ejemplo: Representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.
- **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.
- **Identificación del Riesgo:** Elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Pilar de seguridad de la información, que consiste en la propiedad de 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.
- **Lavado de activos:** Delito que comete toda persona que incurra en alguna de las conductas descritas en el artículo 323 del Código Penal.
- **LA/FT-FPADM:** Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.
- **Listas nacionales e Internacionales:** Relación de personas que de acuerdo con el organismo que las publica, pueden estar vinculadas con actividades de lavado de activos o financiación del terrorismo, como lo son las listas del Consejo de Seguridad de las Naciones Unidas, que son vinculantes para Colombia, OFAC, INTERPOL, Policía Nacional, entre otras.
- **Mapa de Calor:** Herramienta visual empleada para ubicar el nivel de riesgo, a partir del punto de intersección entre su nivel de probabilidad de ocurrencia y su nivel de impacto.
- **Monitoreo:** en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos.
- **Nivel de Riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser: Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
- **Operación Inusual:** Es aquella que realiza una persona natural o jurídica que, por su número, cantidad, o características, no se enmarcan dentro de los sistemas y practicas normales de los negocios de una industria o sector determinado.
- **Operación Intentada:** Se configura cuando se tiene conocimiento de la intención de una persona natural o jurídica de realizar una operación sospechosa, pero no se perfecciona por cuanto quien intenta llevarla a cabo desiste de la misma o porque los controles establecidos o definidos por la persona natural o jurídica no permitieron realizarla.
- **Operación Sospechosa:** Es aquella que por su número, cantidad o características no se enmarca en los sistemas y prácticas normales de los negocios, de una industria o de un sector determinado y, además, que de acuerdo con los usos y costumbres de la actividad que se trate, no ha podido ser razonablemente justificada. Cuando se detecten esta clase de operaciones, deben ser reportadas de manera inmediata a la UIAF.
- **Patrimonio Público:** Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica.
- **Personas expuestas políticamente (PEP'S):** Son las señaladas en el artículo 1 del Decreto 1674 del 21 de octubre de 2016.

D102PR01G01PL03
Versión:01
Fecha: 5/07/2024

- **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.
- **Punto de Riesgo:** Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo.: Aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales.
- **Recurso Público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública, por ejemplo: 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 (Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos)
- **Riesgo de Contagio:** Es la posibilidad de pérdida o daño que puede sufrir el sujeto obligado, directa o indirectamente, por una acción o experiencia de una persona natural o jurídica que posee vínculos con éste.
- **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 LA/FT-FPADM:** Es la posibilidad de pérdida o daño que puede sufrir una persona natural o jurídica, al ser utilizada para cometer los delitos de lavado de activos, financiación del terrorismo o de la proliferación de armas de destrucción masiva.
- **Riesgos asociados al LA/FT – FPAADM:** Son aquellos a través de los cuales se puede llegar a materializar el riesgo de LA/FT- FPAADM, estos son: reputacional, legal, operativo y contagio.
- **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:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo legal:** Es la posibilidad de pérdida o daño, que puede sufrir una persona natural o jurídica al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones, obligaciones contractuales, fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.
- **Riesgo Operativo:** Es la posibilidad de pérdida o daño, que puede sufrir una persona natural o jurídica al incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo reputacional:** Es la posibilidad de pérdida en que incurre una persona natural o jurídica, por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.
- **Riesgo Residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento. Es el resultado de aplicar los controles al riesgo inherente.
- **Riesgo externo:** una situación potencial que pueden generar disrupciones en la organización pero que no están bajo su control.
- **Riesgo emergente:** Son desafíos potenciales que pueden derivarse de cambios que empiezan a aparecer en el entorno, tecnología, regulaciones, o incluso comportamientos sociales.
- **Seguridad de la Información:** Conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión.
- **Segmentación:** Es el proceso por medio del cual se lleva a cabo la separación de elementos en grupos homogéneos al interior de ellos y heterogéneos entre ellos. La separación se fundamenta en el reconocimiento de diferencias significativas en sus características (variables de segmentación).
- **Señales de alerta:** Son todas aquellas situaciones, hechos, eventos, cuantías, indicadores cuantitativos y cualitativos, razones financieras y demás información que de acuerdo con la experiencia y conocimiento de la actividad económica de la persona natural o jurídica, no guardan relación con la misma, o se salen de los parámetros normales.
- **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

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 8 de 41 |

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

5 PRINCIPIOS QUE SOPORTAN LA GESTIÓN DE RIESGOS

Para que la gestión de riesgos sea eficaz, el Ministerio en todos sus niveles debe cumplir con los siguientes principios¹:

- **Integración:** La gestión de riesgos es parte integral de todas las actividades de la organización.
- **Enfoque estructurado y exhaustivo:** Un enfoque estructurado y exhaustivo hacia la gestión de riesgos contribuye a resultados coherentes y comparables.
- **Adaptación:** El marco de referencia y el proceso de la gestión de riesgos se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
- **Inclusión:** La participación apropiada y oportuna de los grupos de valor permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
- **Dinamismo:** Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión de riesgos anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
- **Disponibilidad de mejor información:** Las entradas a la gestión de riesgos se basan en información histórica y actualizada, así como en expectativas. La gestión de riesgos tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
- **Gestión con Factores humanos y culturales:** El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión de riesgos en todos los niveles y etapas.
- **Mejora continua** La gestión de riesgos mejora continuamente mediante aprendizaje y experiencia.

6 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO²

Con el fin de fortalecer el desempeño institucional y aumentar la confianza de las partes interesadas, el Ministerio de Ciencia, Tecnología e Innovación se compromete en identificar y gestionar de manera efectiva los riesgos que puedan afectar el logro de los objetivos institucionales en el marco de los planes, programas y procesos. La entidad, en coherencia con el principio de la debida diligencia establecerá controles para todos los procesos del Sistema Integrado de Gestión (SIG). Adicionalmente, se generarán planes de manejo para los riesgos que se ubican en zona de riesgo residual ALTO o EXTREMO y para todos los riesgos de corrupción o riesgos a la integridad pública.

Para efectos de lo anterior, el Ministerio definirá los lineamientos metodológicos en la **GUÍA PARA LA GESTIÓN DE RIESGOS (D10PR03G01)** en la que se detallan, entre otros aspectos, cómo hacer la identificación, valoración, tratamiento, monitoreo y seguimiento a los riesgos.

6.1 Contenido de la política de administración del riesgo

A continuación, se desarrollan los principales aspectos de la gestión del riesgo institucional, a partir de la Política de Administración del Riesgo:

Tabla 1 Contenido Política Administración del Riesgo

| | |
|--|--|
| Objetivo General | Establecer los lineamientos y criterios para orientar en el Ministerio de Ciencia, Tecnología e Innovación la identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos a los que se enfrenta y que puedan impactar el cumplimiento de los objetivos institucionales en el marco de los procesos, planes y proyectos de la entidad. |
| Alcance | Esta política aplica a todos los procesos establecidos en el marco del Sistema Integrado de Gestión (SIG) del Ministerio de Ciencia, Tecnología e Innovación, bajo los lineamientos metodológicos definidos en la presente guía. |
| Niveles de aceptación al riesgo | <ul style="list-style-type: none"> • Se define tolerar los riesgos que tengan baja probabilidad de ocurrencia y bajo potencial de impacto. • Para el caso de los riesgos residuales (después de controles) cuya calificación se ubique en zona de riesgo ALTO o EXTREMO se debe implementar plan de manejo (tratamiento) para los mismos. • Los riesgos de corrupción o riesgos a la integridad pública son inaceptables, con independencia de la zona de riesgo en la que se ubiquen, por lo que requieren acciones de |

¹ ICONTEC Internacional. (2018). NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31000. GESTIÓN DE RIESGO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

² Aprobada en el marco del Comité de Coordinación del Sistema de Control Interno sesión ordinaria n° 1 fecha 11/04/2024

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 9 de 41 |

| | |
|--|--|
| | manejo que contribuyan a eliminar sus causas. |
| Niveles para calificar el impacto | <ul style="list-style-type: none"> Para la valoración del impacto del riesgo se determinan variables económicas y reputacionales asociadas a los riesgos de gestión, fiscales, seguridad de la información y de TI; así mismo para los riesgos de corrupción se establecen los criterios (19 preguntas) que permiten calificar su impacto. Los niveles para calificar el impacto se describen en el numeral 10.3 y 11.2 de esta guía |
| Tratamiento del riesgo | <ul style="list-style-type: none"> Los riesgos en zona de riesgo residual ALTO o EXTREMO deben implementar plan de manejo al igual que todos los riesgos de corrupción o riesgos a la integridad pública. Las opciones para el tratamiento se describen en el numeral 15 de esta guía |
| Periodicidad para el seguimiento | <ul style="list-style-type: none"> La periodicidad del seguimiento se describe en el numeral 16 de esta guía. |

Fuente: OAPII

Los riesgos relacionados con el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LACFT/FPADM) hacen parte del alcance de la política. Dado que estos riesgos están intrínsecamente vinculados a la corrupción, se gestionarán utilizando la misma metodología que se aplica en la presente Guía para los riesgos de corrupción / riesgos de riesgos a la integridad pública.

7 RESPONSABILIDADES LÍNEAS DE DEFENSA EN EL MARCO DE LA GESTIÓN DE RIESGOS

El Modelo Integrado de Planeación y Gestión (MIPG), en la dimensión 7 “Control Interno” establece roles y responsabilidades para las distintas líneas de defensa para la gestión del riesgo y control, buscando prevenir su materialización a través del siguiente esquema:

Tabla 2 Responsabilidades líneas de defensa

| LÍNEA ESTRATÉGICA DE DEFENSA | |
|--|--|
| Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento. | |
| Responsables: Alta Dirección y el Comité de Coordinación del Sistema de Control Interno | |
| Aspectos Claves | <p>La alta dirección y el equipo directivo, a través de sus comités realizan el seguimiento gerencial a la gestión de riesgos institucional con relación a lo siguiente:</p> <ul style="list-style-type: none"> Revisar los cambios en el Direccionamiento estratégico y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. Hacer seguimiento en el CCSICI a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. 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 en el cumplimiento de los objetivos. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento. Analizar las evaluaciones de la gestión de riesgos, elaboradas por la segunda línea de defensa. Asegurar que los servidores responsables (tanto de la segunda como de la tercera línea de defensa) cuenten con los conocimientos necesarios y que se generen recursos para la mejora de sus competencias Generar recomendaciones para el fortalecimiento de la cultura en la gestión de los riesgos. |

Fuente: OAPII

Tabla 3 Responsabilidades líneas de defensa

| PRIMERA LÍNEA DE DEFENSA | |
|--|--|
| Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. | |
| Responsables: Conformada por: los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad o (jefes, directores, coordinadores u otro cargo). | |
| Aspectos Claves | Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada |

D102PR01G01PL03

Versión:01

Fecha: 5/07/2024

PRIMERA LÍNEA DE DEFENSA

gestión de riesgos, incluyendo los riesgos de corrupción o riesgo a la integridad pública con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos, modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
- Revisión como parte de sus procedimientos de supervisión, la 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 el marco del SIG del Ministerio.
- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, 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 en los medios que disponga la OAPII, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción o riesgos a la integridad pública, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
- Monitorear la ejecución de los controles y reportar la eficacia de estos en la mitigación de los riesgos, conforme a la periodicidad establecida.
- Revisar los planes de mejora establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces, para evitar en lo posible la repetición del evento y lograr el cumplimiento de los objetivos.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de manejo (tratamientos) acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
- Mantener actualizados los mapas de riesgos por procesos.
- Implementar los lineamientos definidos en el marco de Gestión de Riesgos de Seguridad de la Información Institucional.
- Comunicar deficiencias a la Alta Dirección o a las partes responsables para tomar las medidas correctivas, según corresponda.

En cuanto al Monitoreo de Riesgos:

- Líder de proceso:
 - Verificar y aprobar el mapa de riesgos que se cargará al Sistema de Información GINA.
 - Garantizar por parte del proceso la calidad de la información y el reporte oportuno del monitoreo de riesgos, previo a su registro en el sistema de información GINA.
- Agente C4 o responsable del reporte monitoreo:
 - Consolidar y revisar la información reportada
 - Reportar los avances y evidencias en el Sistema de Información GINA.
 - Verificar el cargue de la información reportada
 - Remitir al líder del proceso el reporte oportuno del monitoreo de riesgos, para la validación de calidad.

Fuente: OAPII

Tabla 4 Responsabilidades líneas de defensa

SEGUNDA LÍNEA DE DEFENSA

Soporta y guía a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción o riesgos a la integridad pública, a través del establecimiento de directrices y el apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos; lleva a cabo un seguimiento independiente al cumplimiento de las etapas de la gestión de riesgos.

Responsables: Conformada por los responsables de monitoreo y evaluación de los controles, y gestión del riesgo Jefe de la OAPII, supervisores e interventores contratos o proyectos, responsables de los sistemas de gestión, y Oficial de Seguridad de la Información.

Aspectos Claves

Deben monitorear y revisar el cumplimiento de los objetivos institucionales y de procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción o riesgo a la integridad pública, con relación a lo siguiente:

SEGUNDA LÍNEA DE DEFENSA

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- Analizar el adecuado diseño 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.
- 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 planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos, segunda y tercera línea de defensa con relación a la gestión de riesgos.
- Realizar la difusión de lineamientos, metodologías, roles y responsabilidades para el monitoreo y seguimiento de los mapas de riesgo.

Fuente: OAPII

Tabla 5 Responsabilidades líneas de defensa

TERCERA LÍNEA DE DEFENSA

Provee aseguramiento, evaluación independiente y objetiva sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos, para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como, los riesgos de corrupción o riesgo a la integridad pública.

Responsables: esta línea de defensa está conformada por la Oficina de Control Interno.

Aspectos Claves

Revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través del seguimiento a la adecuada gestión de riesgos a con las siguientes responsabilidades:

- Verificar y evaluar, a través de ejercicios de seguimiento o auditoría interna, la efectividad de los controles, planes de contingencia y planes de tratamiento de los riesgos institucionales, con el fin de:
 - Evaluar la efectividad de los controles en la prevención o mitigación de riesgos.
 - Presentar oportunidades de mejora a la administración en el diseño e implementación de los controles.
 - Mejorar la valoración de los riesgos.
 - Verificar las acciones de monitoreo institucionales.
- Monitorear la exposición al riesgo del Ministerio y realizar recomendaciones con alcance preventivo.
- Asesorar de manera proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos.
- En el evento de materializarse un riesgo de corrupción o riesgo a la integridad pública, es necesario que la OCI realice acciones como:
 - Informar a las autoridades de la ocurrencia del hecho de corrupción o riesgo a la integridad pública.
 - Revisar el mapa de riesgos de corrupción o riesgo a la integridad pública, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción o riesgo a la integridad pública.
- Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre el Sistema de Control Interno.
- Verificar que se realice la actividad de monitoreo por parte de la segunda línea de defensa a los riesgos del Ministerio y brindar, bajo el rol de asesoría y acompañamiento, recomendaciones frente a la administración del riesgo.
- Informar a la alta dirección sobre posibles cambios identificados, que podrían tener un impacto significativo en el Sistema de Control Interno y alertar sobre la probabilidad de riesgo en las dependencias o temas objeto de seguimiento.
- Adelantar seguimiento a la Mapa de Riesgos de corrupción o riesgo a la integridad pública, de acuerdo con la normatividad establecida.

TERCERA LÍNEA DE DEFENSA

- Publicar el informe de seguimiento al Mapa de Riesgos de Corrupción o riesgos a la integridad pública en la página web del Ministerio o en un lugar de fácil acceso para el ciudadano, el cual debe abarcar las siguientes acciones:
 - Verificar la publicación del Mapa de Riesgos de Corrupción o riesgos a la integridad pública en la página web de la entidad.
 - Realizar seguimiento a la gestión del riesgo.
 - Revisar los riesgos y su evolución.
 - Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.
- En el marco de la evaluación independiente se deberán señalar aquellos aspectos que se consideren una amenaza para el cumplimiento de los objetivos de los procesos. En tal sentido el Jefe de control interno debe pronunciarse sobre la pertinencia y efectividad de los controles. También se debe asesorar en la identificación, valoración y gestión de los riesgos fiscales de la entidad y brindar acompañamiento y asesoría en la formulación de controles adecuados tendientes a prevenir efectos dañosos sobre los bienes, recursos e intereses patrimoniales de naturaleza pública.

Fuente: OAPII

Bajo los principios de autocontrol y autogestión, todos los servidores públicos del Ministerio, en el marco de sus funciones y obligaciones son responsables de aplicar mecanismos de control adecuados que busquen mitigar los riesgos a los que están expuestas las labores que le sean designadas, incluso aquellos riesgos que estén enmarcados en sus responsabilidades, pero que no se encuentren especificados en el mapa de riesgos institucional.

8 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS

El aspecto central para el desarrollo y la consolidación de la política de administración de riesgos es la identificación y análisis del mapa de riesgos institucional y la formulación y actualización de la matriz de riesgos (matriz de calor y zonas de riesgo) teniendo en cuenta lo siguiente:

- Los mapas de riesgos deben estar alineados con el Sistema Integrado de Gestión (SIG) y con la planeación estratégica de la entidad.
- Los riesgos residuales ubicados en zona de riesgo alto o extremo podrán tener diferentes tipos de tratamiento “reducir (mitigar, transferir) o evitar” según lo establece la metodología, esto considerando los eventos registrados para dichos riesgos en periodos anteriores. A partir de este análisis todos los riesgos en zona de riesgo alto o extremo deberán tener una propuesta o acción de tratamiento coherente para gestionar el riesgo complementando los controles con otras iniciativas que tengan una temporalidad específica (plan de manejo). T.
- Los riesgos residuales que queden ubicados en zona de riesgo Moderado o Bajo podrán tener cualquiera de los tipos de tratamientos: “aceptar, evitar, reducir”. Si se elige como tratamiento para el riesgo, la opción de “aceptar el riesgo”, significará que para la vigencia no se generarán nuevos planes de acción para mitigar el riesgo. Sin embargo, el que se incluya esta opción **no excluye al líder de proceso de la obligación de continuar aplicando los controles establecidos** y hacer el respectivo seguimiento tanto a los controles ya implementados como a la posible materialización del riesgo. Para riesgos de corrupción o riesgos a la integridad pública no se puede aceptar o asumir el riesgo, así como los riesgos fiscales
- Los mapas de riesgos deben ser aprobados por los líderes de los correspondientes procesos; sin embargo, la Oficina Asesora de Planeación e Innovación Institucional (OAPII) y/o el Comité Gestión y Desempeño Sectorial e Institucional (CGDSI), podrán solicitar que se incluyan en el Mapa de Riesgos, aquellos riesgos potenciales que no hayan sido incluidos por estos.
- Es normal y frecuente que, al analizar un proceso con respecto a los riesgos, los controles y/o planes de manejo no sean ejecutables por el área o áreas que participan en el proceso, puesto que se pueden dar acciones de alcance institucional. Por lo tanto, en el análisis de un proceso se puede identificar la necesidad de emprender acciones que deben liderar otras áreas de la entidad, para lo cual se requerirá el apoyo de la OAPII con el fin de articular estas.
- Los mapas de riesgos deben ser consolidados, publicados y socializados a toda la entidad propendiendo por el desarrollo de la cultura organizacional de gestión de riesgos.
- La actualización de los mapas institucionales de riesgos de gestión se realizará de forma anual según los lineamientos normativos, salvo que por necesidades del servicio se requiera su actualización con otra periodicidad.
- La eliminación de cualquier riesgo deberá ser justificada y aprobada por el líder del proceso; sin embargo, de presentarse justificaciones poco argumentadas, la OAPII deberá pedir ampliación de la justificación hasta tener evidencia de que dicha eliminación no acarreará perjuicios para el Ministerio, para lo cual se podrá solicitar concepto de otros líderes de procesos que puedan dirimir la decisión.
- Teniendo en cuenta el Decreto 1499 del 2022 “Por el cual se adopta la estructura del Ministerio de Ciencia, Tecnología e Innovación, y se dictan otras disposiciones”, conforme con la resolución 2795 de 2022 “Por la cual se

D102PR01G01PL03

Versión:01

Fecha: 5/07/2024

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 13 de 41 |

adopta el nuevo Manual Específico de Funciones y Competencias Laborales de la planta de personal del Ministerio de Ciencia, Tecnología e Innovación”, la Oficina de Tecnologías y Sistemas de Información (OTSI) será la encargada de liderar el proceso de actualización de los riesgos de seguridad de la información a los que se puedan ver expuestos los diferentes procesos de la entidad.

- El Ministerio cuenta con el sistema de información GINA, el cual, mediante su módulo de riesgos, consolida y controla la administración de los riesgos en cada uno de los procesos de la Entidad; este sistema de información se encuentra alineado con la metodología establecida en la presente guía.
- Cada riesgo debe tener un código de acuerdo con su tipología y el proceso al que pertenece teniendo en cuenta la tabla Códigos para la identificación de los riesgos de cada proceso.

Tabla 6 Códigos para la identificación de los riesgos

| | TIPO DE RIESGO | CONSECUTIVO | CÓDIGO DEL PROCESO |
|----------------|---|--------------------|---------------------------|
| | RG – Riesgo de Gestión RC – Riesgo de Corrupción o riesgos a la integridad pública RF – Riesgo Fiscal RSI – Riesgos de Seguridad de la Información RTI – Riesgo de TI | 01 | D102 |
| Ejemplo | Código del Riesgo: RG01-D102 Riesgos de gestión 1 del proceso de Gestión de la Innovación Institucional Fuente: OAPII | | |

Riesgo Reputacional:

La reputación es la evaluación favorable en la mente de las partes interesadas respecto al comportamiento organizacional.

1. Los aspectos determinantes de la reputación son:

- Calidad de la oferta de productos y servicios: se refiere a que la entidad ofrece bienes y servicios que los stakeholders consideren adecuados para la atención de las necesidades y expectativas.
- Orientación al cliente. Se refiere a cómo la entidad trata a las ciudadanías y partes interesadas, más allá de los servicios que genera.
- Resultados y desempeño financiero. Se refiere a la eficiencia en el uso de los recursos financieros: si toma buenas decisiones financieras y entrega información financiera oportuna y adecuada.
- Liderazgo ejecutivo. Se refiere a si la entidad está bien administrada por un líder idóneo y atrayente, con visión de futuro: competencia, carisma, confiabilidad e integridad.
- Calidad como empleador. Un factor que interesa sobre todo a los empleados y al mercado laboral en general. Se refiere a que la entidad sea una buena empleadora, que trate bien y con ecuanimidad a sus trabajadores, con valores profesionales y éticos, preocupada por su bienestar y salud.
- Ética y gobierno corporativo. Tiene que ver con el grado de apertura y transparencia para operar, si se comporta éticamente y si es justa. El público general, las entidades regulatorias, los medios de comunicación y ciertos grupos de activistas suelen ser quienes más se fijan en este aspecto.
- Responsabilidad social, cívica y medioambiental. Implica que la entidad está comprometida con su comunidad a proteger el entorno y apoyar buenas causas — incluyendo hacer esfuerzos para crear puestos de trabajo, o sacrificar ganancias en aras de un medioambiente más limpio.
- Innovación. Se refiere a que la entidad sea creativa, innovadora, ingeniosa, que invierta en investigación y desarrollo, orientada al cambio, pionera en sacar nuevos productos y servicios.

2. Pasos para la Gestión del riesgo reputacional

1. Evaluar la reputación de la entidad entre los stakeholders relevantes, mediante encuestas, entrevistas en profundidad y/o focus group a clientes, servidores, público general, expertos y a otros actores. Analizar estructuralmente los contenidos de los medios de comunicación tanto convencionales (prensa, radio, TV) como sociales (Twitter, Facebook, Instagram, Youtube y otros) porque ellos configuran las percepciones y expectativas de los grupos de interés.
2. Evaluar el "verdadero carácter" de la entidad. Se refiere a evaluar su capacidad efectiva de cumplir con las expectativas de los diferentes públicos, y ser realista al respecto.
3. Minimizar las brechas que existen entre la realidad de la entidad y las percepciones de los stakeholders. No siempre calzan las percepciones de los grupos de interés con la realidad: a veces hay expectativas desmedidas (lo cual es riesgoso), en otros las expectativas están por debajo de la realidad de la organización, en otros hay consistencia entre mal desempeño real y malas percepciones (lo cual solo es revertible mejorando los aspectos mal evaluados primero, y después comunicar esas mejoras —pero no al revés—).

D102PR01G01PL03
Versión:01
Fecha: 5/07/2024

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 14 de 41 |

4. Monitorear los cambios en las creencias y expectativas de los stakeholders. Esto implica tener instalado un sistema de información y monitoreo del entorno.

Por lo anterior, el Ministerio de Ciencia Tecnología e Innovación cuenta con mecanismos diseñados e implementados desde la Oficina Asesora de Comunicaciones para monitorear la percepción de los grupos de valor en el entorno digital y del medio de comunicación. Así mismo, desde el equipo de Atención al Ciudadano se aplica periódicamente una encuesta a usuarios y grupos de interés. Es importante que los resultados de estos ejercicios sean comunicados sistemáticamente.

Riesgos LA/FT – FPADM

La gestión de riesgos relacionados con el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva se incorporará en la metodología de administración de riesgos de corrupción del Ministerio. Esto se logrará mediante la inclusión de estos riesgos en la Política de Administración de Riesgos del Ministerio de Ciencia, Tecnología e Innovación que ya abarca la gestión integral de riesgos de la entidad. Dado que los riesgos asociados al Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva están intrínsecamente vinculados a la corrupción, se gestionarán utilizando la misma metodología que se aplica a los riesgos de corrupción. Esta adaptación de riesgos demuestra el compromiso de Minciencias con el cumplimiento de la metodología establecida en la "Guía para la administración del riesgo y el diseño de controles en las entidades públicas", expedida por el Departamento Administrativo de la Función Pública.

El MinCiencias ha definido como contrapartes para realizar la debida diligencia y el conocimiento a:

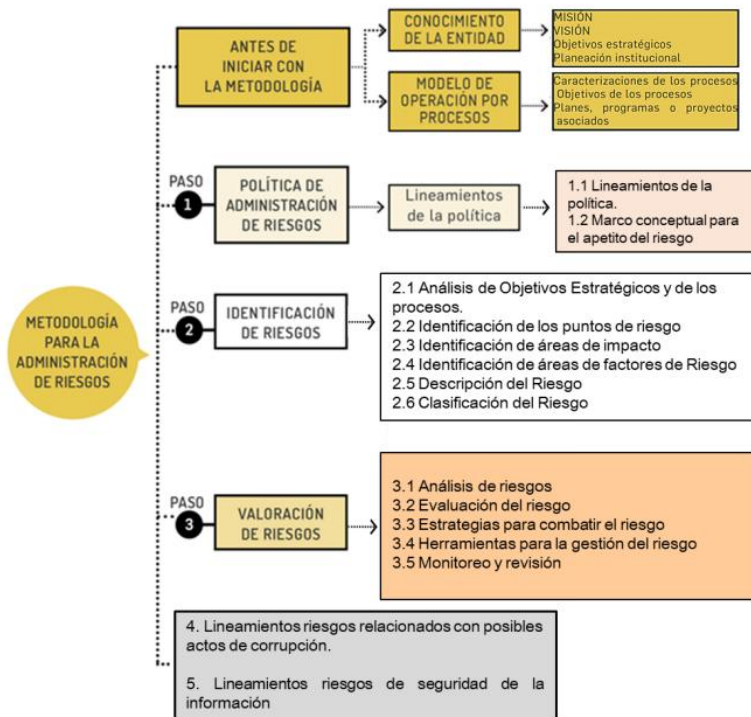
- Proveedores Nacionales e Internacionales de bienes y/o servicios
- Planta de personal
- Terceros beneficiarios de giros en el marco de procesos (beneficiarios de los recursos que administra el Ministerio).

En el caso de generar una relación contractual con o proveedores de bienes y servicios (persona natural y/o jurídica) se realiza la verificación de los requisitos mínimos establecidos en el manual de Contratación.

9 METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

La metodología para la Administración de Riesgos permite al Ministerio establecer los lineamientos a seguir para identificar, analizar, evaluar, monitorear y hacer seguimiento a los riesgos; así como determinar roles y responsabilidades de cada uno de los servidores de la Entidad (esquema de las líneas de defensa) en los riesgos de gestión, corrupción o riesgos a la integridad pública, fiscales y seguridad de la información. Le permite igualmente a la alta dirección de la entidad tener una seguridad razonable en el logro de sus objetivos, para ello, se deben llevar a cabo las actividades descritas para todas las etapas que se relacionan en la siguiente ilustración.

Ilustración 1 Metodología Administración del Riesgo



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

La metodología para la administración de riesgos requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la Entidad, el conocimiento de esta desde un punto de vista estratégico, basado en un esquema de operación por procesos, y la aplicación sistemática de tres (3) aspectos básicos para su desarrollo:

La definición de la **Política de Administración de Riesgos** la cual establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

La **Identificación de riesgos** donde se identifican y reconocen los puntos de riesgo, se identifican áreas de impacto, áreas de factores de riesgo, la descripción del riesgo, la clasificación del riesgo.

La **Valoración del riesgo** donde se establece la probabilidad de ocurrencia del riesgo y el nivel de impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE); así mismo se definen y valoran los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

De otra parte, se hace una breve mención de los lineamientos para el tratamiento de los riesgos relacionados con posibles actos de corrupción, lineamientos a los riesgos de seguridad de la información y riesgos fiscales, temas que en esta guía se mencionan delante de manera más detallada.

9.1 Identificación del Contexto

Esta etapa tiene como propósito identificar y reconocer los riesgos que estén o no bajo el control de la entidad, para ello se debe tener en cuenta el contexto organizacional en el que se desenvuelve la entidad, la caracterización de cada proceso que incorpora elementos esenciales como su objetivo, alcance y también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Para este análisis se pueden tener en cuenta los resultados de la herramienta de diagnóstico integral que se maneja en el proceso de Gestión de la Innovación.

9.1.1 Análisis de objetivos

Los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso

Tabla 7 Análisis de Objetivos

| Análisis de los Objetivos Estratégicos | Análisis de los Objetivos del Proceso |
|--|---|
| <p>La entidad debe analizar la planeación estratégica e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.</p> <p>Es necesario revisar que la planeación estratégica se encuentre alineada con la Misión y la Visión Institucional, así como, analizar su adecuada formulación.</p> | <p>Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero, además se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos</p> |

Fuente: Guía para la administración del riesgo y el diseño de controles, V6 DAFP

9.1.2 Establecimiento del contexto

El contexto se relaciona con las condiciones internas y externas que pueden generar eventos que afecten negativa o positivamente el cumplimiento de la misión y objetivos del Ministerio, por lo tanto, para su construcción es fundamental partir de la misión, los objetivos, el plan estratégico, y la naturaleza misma de la Entidad. Cada uno de los procesos debe determinar el contexto para lo cual puede utilizar la herramienta DOFA. El contexto organizacional podrá consultarse en el sistema de información GINA.

9.2 Identificación de los puntos de riesgo

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

9.3 Identificación de áreas de impacto

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

9.4 Identificación de áreas de factores de riesgo

Para la identificación de los riesgos es importante revisar las dependencias o procesos que son susceptibles de ser factores generadores de riesgos, definidos como aquellas actividades del proceso que pueden ser críticas para el logro del objetivo propuesto o donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo. En la siguiente tabla se detalla un listado con ejemplos de factores de riesgo que puede tener el Ministerio:

Tabla 8 Factores de Riesgo

| Factor | Definición | Descripción |
|-----------------|---|---|
| Procesos | Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización. | Falta de procedimientos |
| | | Ausencia de divulgación de los procedimientos |
| | | Errores de grabación, autorización |
| | | Errores en cálculos para pagos internos y externos |
| | | Falta de capacitación, temas relacionados con el personal |
| Talento Humano | Incluye seguridad y salud en el trabajo. | Hurto de activos |
| | Se analiza posible dolo e intención frente a la corrupción. | Posibles comportamientos no éticos de los empleados |
| | | Fraude interno (corrupción, soborno) |
| Tecnología | Eventos relacionados con la infraestructura tecnológica de la entidad | Daño de equipos |
| | | Caída de aplicaciones |
| | | Caída de redes |
| | | Errores en programas |
| Infraestructura | Eventos relacionados con la infraestructura física de la entidad | Derrumbes |
| | | Incendios |
| | | Inundaciones |
| | | Daños a activos fijos |
| Evento externo | Situaciones externas que afectan la entidad. | Suplantación de identidad |
| | | Asalto a la oficina |
| | | Atentados, vandalismo, orden público |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

9.5 Identificación de riesgos

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

9.5.1 Técnicas para la identificación de riesgos

La identificación de riesgos se realiza determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos del proceso o de los objetivos estratégicos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o estratégicos.

Las preguntas claves para la identificación del riesgo permiten determinar:

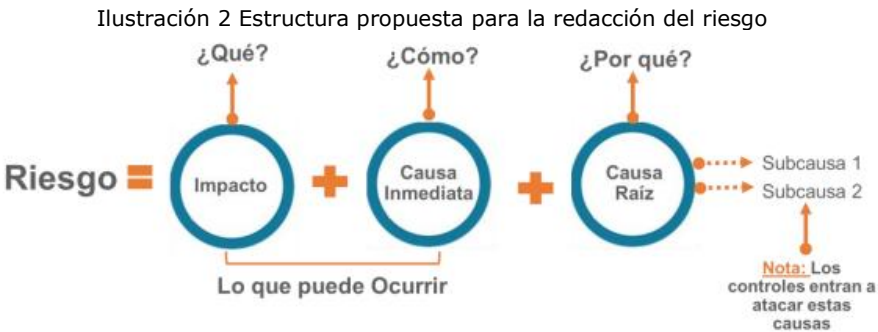
- **¿QUÉ PUEDE SUCCEDER?** Identificar la afectación del incumplimiento del objetivo estratégico o del proceso según sea el caso, en términos de impacto económico o reputacional.
- **¿CÓMO PUEDE SUCCEDER?** Establecer las causas inmediatas a partir de los factores determinados en el contexto.
- **¿POR QUÉ PUEDE SUCCEDER?** Determinar o establecer la causa raíz de acuerdo con el desarrollo del objetivo del proceso.

En términos generales para la identificación y descripción de un riesgo se deben incluir todos los detalles que se consideren necesarios y que sean de fácil entendimiento tanto para el líder como para persona ajenas al proceso.

10 RIESGOS DE GESTIÓN

10.1 Descripción del Riesgo

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



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

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

Al desglosar la estructura propuesta se tiene:

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

En general, para identificar y definir correctamente un riesgo se debe **evitar** lo siguiente:

- Iniciar con palabras negativas como: “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...”
- Generar al lector o escucha la imagen del evento como si ya estuviera sucediendo.
- Describir riesgos usando omisiones o desviaciones del control, por ejemplo: Errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- Describir causas como riesgos. **Ejemplo:** Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- Describir riesgos como la negación de un control. **Ejemplo:** Retraso en la prestación del servicio por no contar con digiturno para la atención.
- Categorizar riesgos como transversales, lo que pueden existir son causas transversales. **Ejemplo:** Pérdida de expedientes.
- Ubicar en la causa inmediata lo que es una causa raíz o identificar riesgos que no tienen conexión con el objetivo del proceso. Si el objetivo del proceso es “adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación” un riesgo puede ser: “Posible pérdida económica por interrupciones recurrentes de la operación debido a la inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad”

Desagregando la estructura propuesta en el párrafo precitado y para dar mayor comprensión, en el siguiente ejemplo se puede observar cómo quedaría pormenorizado este riesgo:

Tabla 9 ejemplo descripción riesgo

| | |
|---|--|
| Proceso: | Gestión de recursos. |
| Objetivo del Proceso: | adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación. |
| Alcance: | inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisidores) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas. |
| Atendiendo el esquema propuesto para la redacción del riesgo, tenemos: | |
| Redacción inicia con: | Posibilidad de |
| Impacto ¿Qué? | afectación económica |
| Causa Inmediata ¿Cómo?: | interrupciones recurrentes de la operación |
| Causa Raíz ¿Por qué? | debido a la inoportuna adquisición de los bienes y servicios requeridos por la entidad |

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 DAEP.

10.2 Clasificación del Riesgo

Permite agrupar los riesgos identificados. Se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 10 Clasificación de riesgos

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

| Clasificación | Descripción |
|------------------|-------------|
| Eventos externos | |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

Ilustración 3 Relación entre los factores de riesgo y clasificación del riesgo



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

10.3 Valoración del Riesgo

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

Los elementos que desarrollan la valoración del riesgo son el análisis de los riesgos (zona de riesgo inicial: Riesgo Inherente) y su evaluación (zona de riesgo final: Riesgo Residual), elementos que se describen a continuación:

Análisis de riesgos: Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

- **Probabilidad de ocurrencia del riesgo:** La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo. Así las cosas, la probabilidad inherente será el número de veces que se pasa por el punto del riesgo en el periodo de 1 año, en la siguiente tabla se establecen los criterios para definir el nivel de probabilidad.

Tabla 11 Criterios para definir el nivel de probabilidad

| Descriptor | 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 mínimo 501 veces al año y máximo 5.000 veces por año | 80% |
| Muy Alta | La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año | 100% |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

- **Niveles para calificar el Impacto:** Se definen los impactos económicos y reputacionales como las variables principales para establecer los criterios que determinan el nivel de impacto.

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

La siguiente tabla muestra los criterios establecidos en la Guía del DAFP para definir el nivel de impacto:

Tabla 12 Criterios para definir el nivel de impacto

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

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

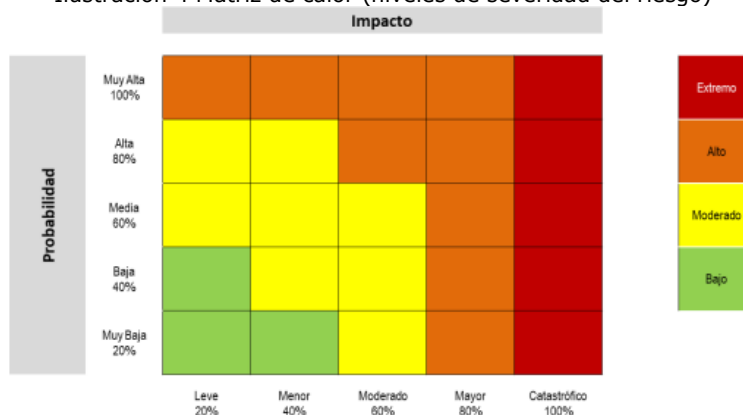
Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto. Por ejemplo: para un riesgo identificado se define un impacto económico en nivel leve e impacto reputacional en nivel moderado, **se tomará el más alto**, en este caso sería el nivel moderado.

10.4 Evaluación del Riesgo

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos se busca determinar la zona de riesgo inicial (también conocido como **RIESGO INHERENTE**).

- **Análisis preliminar (riesgo inherente):** Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definió 4 zonas de severidad en una matriz de calor, así:

Ilustración 4 Matriz de calor (niveles de severidad del riesgo)



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

El eje X (horizontal) muestra el **impacto** y el eje Y (vertical) la **probabilidad** de ocurrencia. La intersección de los datos de probabilidad e impacto corresponde al nivel de riesgo inicial o inherente. Los colores hacen visible qué tan crítico es el riesgo en términos cualitativos, ubicando la intersección en **verde** si es **Bajo**, **amarillo** si es **Moderado**, **naranja** si es **Alto** o **rojo** si es **Extremo**.

Esta valoración del riesgo se hace con el fin de establecer prioridades para su manejo y tomar decisiones en cuanto a su tratamiento.

La forma de llevar a cabo esta valoración consistirá en presentar a los servidores que por su conocimiento del proceso se consideren expertos, los riesgos identificados (riesgo, causas y consecuencias) para que revisen detalladamente esta información. A continuación, el servidor seleccionará la probabilidad de ocurrencia para cada una de las causas y un valor de impacto general para el riesgo, según su conocimiento y experticia.

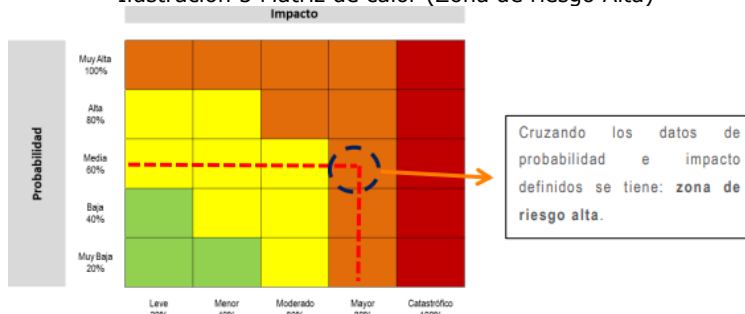
Por ejemplo, para un riesgo determinado, se obtiene la siguiente valoración, en términos de probabilidad de ocurrencia, e impacto:

Probabilidad Inherente: Media 60%

Impacto Inherente: Mayor 80%

Al cruzar los datos de probabilidad e impacto definidos, se tiene: zona de riesgo alta, tal como se muestra a continuación:

Ilustración 5 Matriz de calor (Zona de riesgo Alta)



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

10.5 Valoración de Controles

A partir del análisis del riesgo inicial, se identifica e implementa una o más acciones específicas, denominadas **controles**, que contribuyan a modificar la exposición al riesgo, ya sea en la valoración de probabilidad de impacto o en la valoración de impacto.

10.5.1 Estructura para la descripción del control

La estructura básica de un control consta de los siguientes elementos:

1. Responsable. Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
2. Periodicidad. Debe tener una periodicidad (diario, mensual, trimestral, anual) etc. definida para su ejecución.
3. Propósito. Se determina mediante verbos que indican la acción (**verificar, validar, conciliar, comparar, revisar, cotejar**), que deben realizar como parte del control.
4. ¿Cómo se realiza el control? Corresponde a los detalles que permiten identificar claramente el objeto del control.
5. Observaciones y desviaciones. Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
6. Evidencia de la ejecución del control.

Ej-mplo:

El -(1) **PROFESIONAL DE CONTRATACIÓN** - (2- **CADA VEZ** - que se va a realizar un contrato, (3) **VERIFICA QUE LA INFORMACIÓN SUMINISTRADA POR EL PROVEEDOR CORRESPONDA CON LOS REQUISITOS ESTABLECIDOS DE CONTRATACIÓN**, - (4) **A TRAVÉS DE UNA LISTA -E CHEQUEO** - donde están los requisitos de información y la revisión con la información física suministrada por el proveedor. (5) **EN CASO DE ENCONTRAR INFORMACIÓN FALTANTE, REQUIERE AL PROVEEDOR A TRAVÉS DE CORREO PARA EL SUMINISTRO DE LA INFORMACIÓN** y poder continuar con el proceso de contratación. (6) **COMO EVIDENCIA queda** la respectiva lista de chequeo diligenciada con la información de la carpeta del cliente y los correos solicitando la información faltante en los casos en que aplique.

10.5.2 Tipologías y atributos para el diseño de los controles

Teniendo en cuenta las características relacionadas con la eficiencia y la formalización, se tienen las siguientes tipologías de controles:

- **Control Preventivo**: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se dirige hacia las causas del riesgo, para establecer las condiciones que aseguren el resultado final esperado. Ataca la probabilidad de ocurrencia del riesgo. Dentro de la tipología de controles esta es la más eficientes.
- **Control Detectivo**: Control accionado durante la ejecución del proceso o de la actividad que puede generar el riesgo. Los controles de este tipo detectan el riesgo, pero generan reproceso. Atacan la probabilidad de ocurrencia del riesgo

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 22 de 41 |

- **Control Correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Permiten reducir el impacto de la materialización del riesgo. Los controles de este tipo tienen costos implícitos.

De acuerdo con la forma como se ejecutan tenemos:

- **Control Manual:** Controles que son ejecutados por personas, tienen implícito el error humano.
- **Control 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.

Tabla 13 Atributos para el diseño del Control

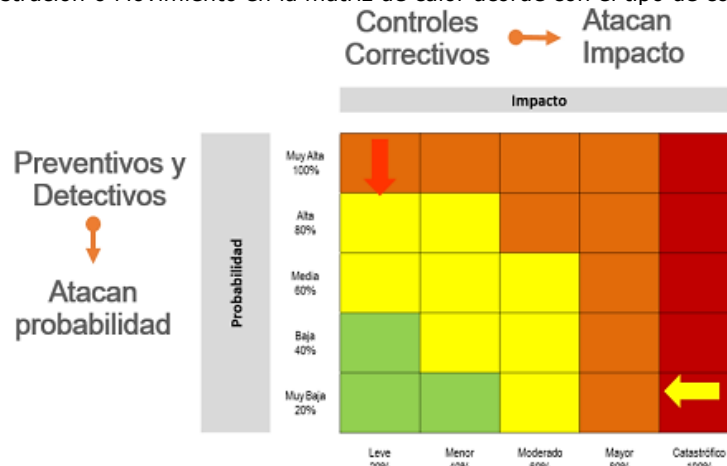
| Características | | | Descripción | Peso |
|-------------------------|----------------|----------------|--|------|
| Atributos de eficiencia | Tipo | Preventivo | Va hacia las causas del riesgo, aseguran el resultado final esperado. | 25% |
| | | Detectivo | Detecta que algo ocurre y devuelve el proceso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

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

Cada control identificado deberá ser valorado en términos de su efectividad sobre el riesgo, de tal forma que para cada control será necesario analizar sus atributos, teniendo en cuenta las características relacionadas con la eficiencia y la formalización, a fin de determinar si modifica la variable de probabilidad de ocurrencia, a la variable de impacto o ambos.

Entre más fuertes sean los controles, mayor será la variación entre el riesgo inherente y el riesgo residual, como se observa en la ilustración 6 que muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 6 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 – V6 DAFP

Con base en lo anterior, se puede afirmar que un riesgo inherente que esté en zona extrema por tener alto impacto y alta probabilidad de ocurrencia puede cambiar a una zona de riesgo residual de impacto moderado y de probabilidad baja después de aplicar controles preventivos, automáticos y documentados.

Nota: Para mayor comprensión del análisis y evaluación de los controles, remitirse a la Guía para la administración del riesgo y el diseño de controles en entidades públicas (versión 6), emitida por el Departamento Administrativo de la Función Pública, numeral 3.2.2.3., en el cual se describen unos ejemplos con los que se indica cómo se determina el nivel de riesgo (riesgo residual), descrito como el resultado de aplicar la efectividad de los controles al riesgo inherente o riesgo inicial.

10.6 Determinación del riesgo residual

Una vez se determinan los controles existentes y se realiza la valoración de estos, se desarrollan los cálculos que permiten obtener el riesgo residual, el cual surge como resultado de la eficacia de estos controles, se toma un ejemplo propuesto donde se observan los cálculos requeridos para la aplicación de los controles:

Tabla 14 Aplicación de controles para establecer el riesgo residual

| Riesgo | Datos relacionados con la probabilidad e impacto inherentes | | Datos valoración de controles | | Cálculos requeridos |
|--|---|-------|---------------------------------|-----|--|
| | Probabilidad Inherente | | Valoración control 1 preventivo | | |
| Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos | | 60% | | 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% | | | |
| | Impacto Inherente | 80% | | | |
| | No se tienen controles para aplicar al impacto | N/A | N/A | N/A | N/A |
| | Impacto Residual | 80% | | | |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

Es necesario considerar que para los de corrupción o riesgos a la integridad pública únicamente hay disminución de probabilidad, puesto que, como ya se indicó en la valoración del impacto, para este tipo de riesgos no se consideran riesgos leves o menores. Es decir, para el impacto no opera el desplazamiento.

11 RIESGOS DE CORRUPCIÓN O RIESGOS A LA INTEGRIDAD PÚBLICA

11.1 Descripción del Riesgo

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

“Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes No.167 de 2013).

Es necesario que en la descripción del riesgo de corrupción o riesgos a la integridad pública concurren los componentes de su definición, así:

Tabla 15 Estructura propuesta para la redacción del riesgo

| MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN | | | | |
|---|------------------|---------------|----------------------------------|-------------------|
| Descripción del riesgo | Acción u omisión | Uso del poder | Desviar la gestión de lo público | Beneficio privado |
| Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato. | X | X | X | X |

Fuente: Secretaría de Transparencia de la Presidencia de la República

Nota: A diferencia de los riesgos de gestión en los riesgos de corrupción o riesgos de integridad pública los elementos de la descripción de la estructura pueden ir en distinto orden de acuerdo con la necesidad del proceso.

11.2 Valoración del Riesgo de Corrupción o riesgo a la integridad pública

- **Análisis de la probabilidad:** Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda. El Ministerio para unificar el criterio de calificar la probabilidad toma como referencia la descripción utilizada para los riesgos de gestión.

Tabla 16 Criterios para calificar la probabilidad

| Descriptor | 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 mínimo 501 veces al año y máximo 5.000 veces por año | 80% |
| Muy Alta | La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año | 100% |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

- **Análisis del Impacto:** El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Tabla 17 Criterios para calificar el impacto en riesgos de corrupción

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

**Nivel de
impacto
MAYOR**

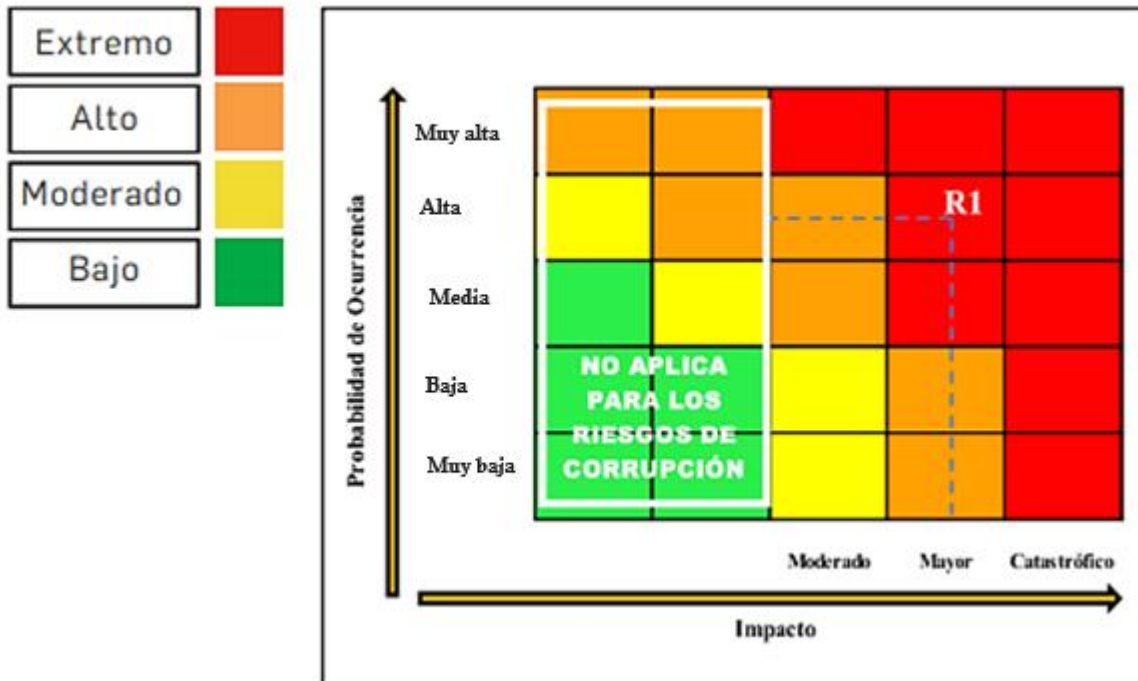
Fuente: Secretaría de Transparencia de la Presidencia de la República

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

11.3 Evaluación del Riesgo de Corrupción o riesgo a la integridad pública

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (también conocido como RIESGO INHERENTE).

Ilustración 7 Matriz de calor (niveles de severidad del riesgo)



Fuente: Construcción Propia

11.4 Valoración de Controles

Aplicar lo definido en el numeral 10.5

11.5 Determinación del riesgo residual

Aplicar lo definido en el numeral 10.6

12 RIESGOS FISCALES

Tienen como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado.

12.1 Identificación del Riesgo

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas. (Ver anexo 1)

12.2 Descripción del Riesgo

Se describen los elementos que componen la definición de Riesgo Fiscal:

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

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



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

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

Al desglosar la estructura propuesta se tiene:

- **Impacto:** Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- **Circunstancia inmediata:** Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
- **Circunstancia raíz:** Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

Ejemplo:

Proceso: Gestión de Recursos

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

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

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

Redacción inicia con: Posibilidad de

Impacto - ¿Qué?: Efecto dañoso sobre bienes públicos

Circunstancia Inmediata - ¿Cómo?: Por pérdida, extravío o hurto de bienes muebles de la entidad.

Circunstancia Raíz - ¿Por qué?: A causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Tabla 18 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

| Bienes Públicos | Recursos públicos | Intereses patrimoniales de naturaleza pública |
|---|---|---|
| Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas. | Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura. | Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato. |
| Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas. | Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado. | Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

12.3 Valoración del Riesgo Fiscal

Se busca establecer la probabilidad inherente de ocurrencia del Riesgo Fiscal y sus consecuencias o impacto inherentes.

- **Determinar la probabilidad:** Se entiende como la posibilidad de ocurrencia del Riesgo Fiscal.

Se determina según al número de veces que se pasa por el punto de Riesgo Fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen Gestión Fiscal. (Ver tabla 5).

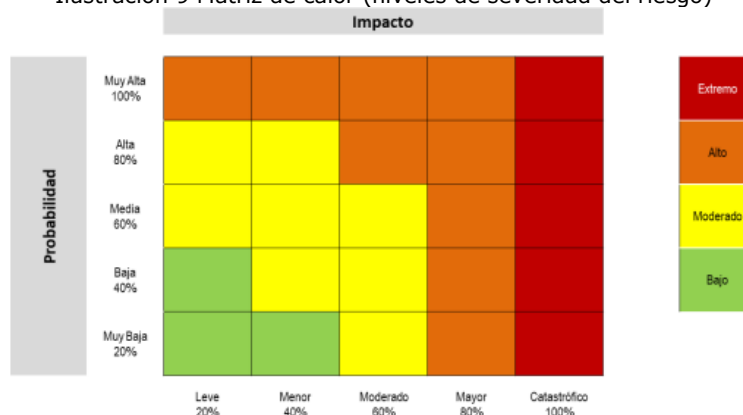
- **Niveles para calificar el Impacto:** Considerando la naturaleza y alcance del Riesgo Fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal (ver tabla 6)

- **Determinar el Riesgo Inherente**

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

Ilustración 9 Matriz de calor (niveles de severidad del riesgo)



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 29 de 41 |

El cruce entre la probabilidad y el impacto indicará en que zona se encuentra el riesgo inherente (Bajo, Moderado, Alto, Extremo).

12.4 Valoración de Controles

Aplicar lo definido en el numeral 10.5.

12.5 Determinación del riesgo residual

Aplicar lo definido en el numeral 10.6

13 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para el caso de los riesgos sobre seguridad de la información, se debe realizar la incorporación del Anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en Entidades públicas”, de manera tal que los responsables analicen y establezcan, en el marco de sus procesos, los activos de información asociados y se identifiquen los riesgos correspondientes.

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”. Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Le corresponde a la primera línea de defensa identificar los activos en cada proceso.

13.1 Identificación de los activos de seguridad de la información

Un activo, es cualquier elemento que tenga valor para la Entidad, sin embargo, en el contexto de seguridad de la información, son activos elementos tales como: aplicaciones de la Entidad, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO que utiliza la Entidad para funcionar en el entorno digital. Así la Entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital³.

Los activos de Información la Entidad pueden ser consultados con el Oficial de Seguridad en la “Matriz de inventarios de activos de información de TI” D103M02F01. Para realizar la identificación de activos relacionados con seguridad de la información, deberá tenerse en cuenta la sección 3.1.6 del a Anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en Entidades públicas”, del Ministerio de Tecnologías de la Información y las Comunicaciones.

13.2 Identificación del riesgo de seguridad de la información

En la identificación de las amenazas es necesario tener en cuenta cuáles y cuántos activos de información tiene cada proceso bajo su responsabilidad. Es importante considerar que las amenazas pueden causar daño temporal o permanente a los activos, procesos y sistemas de soporte de la Entidad. Algunas amenazas pueden afectar a más de un activo y pueden causar diferentes impactos dependiendo de los activos que se vean afectados. (Ver “Manual de inventario de activos, clasificación y publicación de la información” Código D103M02).

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información ⁴:

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

De acuerdo con lo definido en la “Guía para la administración del riesgo y el diseño de controles en Entidades públicas” versión 06, para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 “Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas” donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

³ FUNCIÓN PÚBLICA. Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Bogotá, 2020. Página. 75

⁴ Ibíd. Página. 78

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 30 de 41 |

Las vulnerabilidades son fallas o debilidades que afectan la confidencialidad, integridad y disponibilidad de los sistemas. La identificación podrá obtenerse de pruebas de vulnerabilidad, visitas, entrevistas y/o basados en los criterios que la Entidad vea necesarios. Asimismo, es importante tener en cuenta que, la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Las posibles amenazas y vulnerabilidades que ocasionan la aparición de un riesgo sobre un activo de información se relacionan a continuación, teniendo en cuenta el tipo de activo:

Tabla 19 Ejemplos Vulnerabilidades y Amenazas por tipo de activo

| TIPO DE ACTIVO | EJEMPLO DE VULNERABILIDADES | EJEMPLO DE AMENAZAS |
|----------------|--|---|
| HARDWARE | Mantenimiento insuficiente | Incumplimiento en el mantenimiento del sistema de información |
| | Ausencia de esquemas de reemplazo periódico | Destrucción de equipos o medios |
| | Ausencia de un eficiente control de cambios en la configuración | Error en el uso |
| | Susceptibilidad a las variaciones de temperatura | Pérdida del suministro de energía |
| | Almacenamiento de medios sin protección | Hurto de medios o documentos |
| SOFTWARE | Ausencia de parches de auditoria | Abuso de derechos |
| | Ausencia de documentación | Error en el uso |
| | Tablas de contraseñas sin protección | Falsificación de derechos |
| | Ausencia de control de cambios eficaz | Manipulación con software |
| RED | Arquitectura de red insegura | Espionaje remoto |
| | Envío de contraseñas en texto claro | Espionaje remoto |
| | Gestión inadecuada de la red | Saturación del sistema de información |
| PERSONAL | Ausencia de personal | Incumplimiento en la disponibilidad del personal |
| | Falta de conciencia acerca de la seguridad | Error en el uso |
| | Ausencia de políticas para el uso correcto del correo electrónico | Uso no autorizado del equipo |
| ENTIDAD | Ausencia de auditorias | Abuso de derechos |
| | Ausencia de procedimiento formal para el registro y retiro de usuarios | Abuso de derechos |
| | Ausencia de procedimientos de control de cambios | Incumplimiento en el mantenimiento del sistema de información |
| | Ausencia de procedimientos para el manejo de la información | Error en el uso |

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

13.3 Valoración del riesgo de seguridad de la información

Para esta etapa se deben aplicar los lineamientos de medición de la probabilidad e impacto definidos en la sección 10.3 de la presente guía.

13.4 Controles asociados a la seguridad de la información

Para mitigar/tratar los riesgos de Seguridad de la información el Ministerio de Ciencia, Tecnología e Innovación aplica los criterios establecidos para la definición de controles del Anexo A de la norma ISO 27001:2013, los cuales también se encuentran en estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas".

14 GESTIÓN DE RIESGOS DE TI

Los lineamientos desarrollados en este ítem aplican para los proyectos del Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI. El proceso de identificación y gestión de los Riesgos de TI debe asegurar que no exceden el apetito ni la tolerancia al riesgo institucional de acuerdo con lo definido en la presente guía, y deben tratarse los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales, según lo definido en el numeral 15 Tratamiento del Riesgo

D102PR01G01PL03
Versión:01
Fecha: 5/07/2024

Un escenario de riesgo describe un evento relacionado con TI que puede llevar a un impacto en la Entidad. Para que los escenarios de riesgo sean completos y se puedan utilizar en análisis de riesgos, deben contener los siguientes componentes, que se muestran a continuación.

Tabla 20 Componentes del Escenario de Riesgos de TI

| | | |
|-----------------------------|-------------------------|---|
| Escenario del Riesgo | Actor | <ul style="list-style-type: none"> • Interno (Funcionarios, contratistas) • Externo (aliado estratégico o proveedor de TI) |
| | Tipo de amenaza | <ul style="list-style-type: none"> • Malicioso • Accidental • Fracaso • Natural |
| | Acción | <ul style="list-style-type: none"> • Divulgación • Interrupción • Modificación • Robo • Destrucción • Diseño ineficaz • Ejecución ineficaz • Regulación • Uso inadecuado |
| | Activo / Recurso | <ul style="list-style-type: none"> • Personas • Ministerio • Procesos • Infraestructura (Instalaciones, Infraestructura de TI) • Arquitectura de Componentes Institucionales (Información, Tecnología, Aplicaciones) |

Fuente: Elaboración propia según ISACA (2009)

En relación con los riesgos de TI se deben llevar a cabo las siguientes actividades:

a) Evaluar la gestión de riesgos:

- Establecer el nivel de riesgos de TI que la Entidad está dispuesta a asumir para el cumplimiento de los objetivos estratégicos (apetito del riesgo).
- Evaluar factores de riesgos de TI con anterioridad a la toma de decisiones estratégicas, y dar a conocer a la alta dirección, para que éstas se tomen siendo conscientes de los posibles riesgos.
- Evaluar si el uso de las TI tiene una evaluación y valoración del riesgo adecuada.
- Evaluar actividades de gestión del riesgo de TI para garantizar su alineación con las capacidades institucionales.

b) Orientar la gestión de riesgos:

- Promover una cultura de gestión de riesgos de TI
- Identificar de manera proactiva los riesgos de TI, las oportunidades e impactos potenciales para la Entidad.
- Orientar la integración de la gestión de riesgos de TI y la operación y toma de decisiones institucional.
- Elaborar el plan de comunicación y planes de acción de gestión de riesgos de TI
- Definir y orientar la implementación de mecanismos de respuesta ante riesgos de TI cambiantes, y su notificación.
- Los riesgos de TI, las oportunidades, los problemas y preocupaciones pueden ser notificados por cualquier persona y en cualquier momento.
- El riesgo de TI debe ser gestionado de acuerdo con las políticas definidas para tal fin.
- Identificar objetivos e indicadores claves de gobierno y gestión de riesgos, y definir métodos para su medición.

c) Supervisar la gestión de riesgos

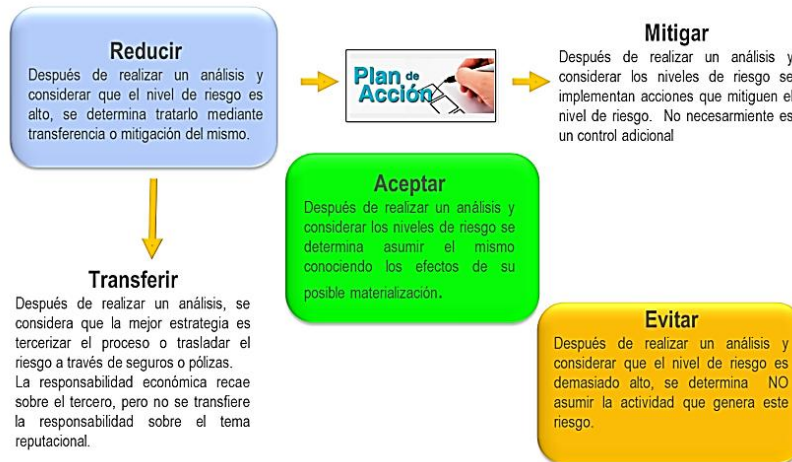
- Supervisar la gestión del riesgo de TI
- Supervisar metas y métricas de gobierno y gestión de riesgos de TI respecto a los objetivos institucionales.
- Informar problemas en la gestión de riesgos al Comité Gestión y Desempeño Sectorial e Institucional

15 TRATAMIENTO DEL RIESGO

Consiste en decidir cómo actuar frente a un determinado nivel de riesgo, esta decisión puede ser ACEPTAR, REDUCIR O EVITAR.

En la siguiente ilustración se aprecia las estrategias opciones de manejo y su relación con la necesidad de definir planes de manejo en el mapa de riesgos.

Ilustración 10 Estrategias para combatir el riesgo



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

Los líderes de proceso deben evaluar las opciones existentes en materia de tratamiento de riesgo, partiendo de la política de administración de riesgos y teniendo en cuenta su importancia, los efectos que puede tener sobre la entidad, su probabilidad e impacto y la relación costo-beneficio de las medidas de tratamiento. El tratamiento es una decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al Riesgo Residual.

Las opciones para el tratamiento del riesgo son:

- **ACEPTAR EL RIESGO:** Asumir el mismo conociendo los efectos de su posible materialización.
- **REDUCIR EL RIESGO:** Se determina tratarlo mediante transferencia o mitigación de este.
- **EVITAR EL RIESGO:** Se determina NO asumir la actividad que genera este riesgo.

Estrategia de reducción del riesgo

- **TRANSFERIR:** 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. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
- **MITIGAR:** Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo.

15.1 Plan de manejo de riesgo

Conjunto de actividades que complementan los controles y que agregan valor a gestión preventiva y a la debida diligencia. Para desarrollar el tratamiento de un modo más específico, se debe consolidar un plan de manejo, el cual debe ser detallado en función del riesgo y sus causas. Se debe determinar en este plan:

- **Actividades:** Las acciones para el tratamiento del riesgo describen las actividades que se deben implementar para su mitigación, se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios en la infraestructura, entre otras. Las actividades tienen que ser concretas, tener temporalidad específica y deben contar con medios de verificación. Es importante tener mínimo una (1) actividad, máximo tres (3) actividades que complementen los riesgos)
- **Responsables:** Son los roles y/o personas responsables de llevar a cabo las actividades específicos que componen el plan de acción, estos deben tener el debido empoderamiento que permita asegurar que la acción se ejecute adecuadamente.
- **Las fechas de ejecución.** Se debe enlistar para cada actividad, el lapso tiempo mínimo y máximo para la implementación de las actividades o las frecuencias de aplicación de estas.
- **Evidencias o soportes del plan de manejo:** Se deben determinar las evidencias que permitan verificar de modo objetivo el cumplimiento de la acción, estas deben estar totalmente relacionadas a las acciones, puesto que es el modo en que estas son materializadas.

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 33 de 41 |

16 MONITOREO Y SEGUIMIENTO DE RIESGOS

16.1 Consideraciones generales para el Monitoreo de Riesgos

Una vez diseñado y validado el mapa de riesgos, es necesario su monitoreo, teniendo en cuenta que estos nunca dejan de representar una amenaza. Para el Ministerio esta actividad es de gran importancia y está a cargo de los líderes de los procesos en conjunto con sus equipos, su monitoreo es esencial para asegurar la eficiencia en la administración de los riesgos.

Para el Ministerio, el monitoreo es permanente y no se limita a los informes de segunda y tercera línea. Para esto se debe considerar la capacidad de acceder a las evidencias de los controles y planes de manejo (tratamiento), así como la periodicidad de cada una de estas, ya sean con cortes fijos de fechas o con frecuencias mensuales, trimestrales, cuatrimestrales, semestrales o anuales, dependiendo el caso. El monitoreo debe verificar las evidencias de los controles y planes de manejo (tratamientos) tal y como fueron planificados, permitiendo así concluir objetivamente si la actividad se realizó adecuadamente y si fue eficaz

El monitoreo debe realizarse en el Sistema de Información GINA, a través del módulo de riesgos, en el campo de Monitoreo. Para el monitoreo, el proceso podrá asignar como responsables del reporte y cargue de evidencias de los controles y planes de tratamiento a los Agentes C4 u otros responsables.

En esta fase el líder del proceso junto con su equipo como primera línea de defensa debe:

- Validar que los controles son eficaces tanto en el diseño como en la operación.
- Mejorar o definir nuevos controles
- Obtener información adicional que permita mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
- Identificar lecciones aprendidas
- Detectar cambios en el contexto interno y externo.
- Identificar riesgos emergentes y evaluar su inclusión al mapa de riesgos
- Seguimiento a la ejecución de los tratamientos

Estas actividades permiten determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los factores de riesgo, así como su identificación, análisis y valoración.

16.2 Acciones a seguir en caso de Materialización del Riesgo

La posibilidad de materialización de un riesgo siempre está latente en el giro ordinario de cualquier actividad, sea ésta realizada por una organización, un conglomerado, una sociedad o una persona; en esas condiciones lo que se debe hacer es estar alerta permanentemente, revisar procesos, procedimientos, controles, riesgos, objetivos, etc., sin embargo y pese a los esfuerzos realizado un riesgo se puede materializar, y por supuesto el Ministerio no es la excepción, razón por la cual se debe actuar lo más pronto posible para mitigar el impacto que este genera y evitar su repetición. En ese orden de ideas a continuación, se indican las actividades que deben llevarse a cabo de manera prioritaria en el indeseado escenario de un evento que conlleve inevitablemente a la materialización de un riesgo.

Tabla 21 Actividades Materialización del Riesgo

| TIPO DE RIESGO | LÍNEA DE DEFENSA | CONDUCTO REGULAR | ACTIVIDADES |
|--------------------|------------------|--|--|
| Riesgos de gestión | Primera línea | Jefes de área o Líder del proceso y su equipo de trabajo | <ul style="list-style-type: none"> • Implementar el plan de contingencia, documentarlo y reportar en el Sistema de Información GINA el evento o materialización del riesgo con sus evidencias. • Análisis de la materialización con sus causas en mesa de trabajo con la OAPII. • Atender la situación a través de correcciones y/o haciendo frente a las posibles consecuencias. • Revisar el mapa de riesgos, en particular, las causas, riesgos y controles existentes y los planes de manejo (tratamiento). • Revisar el contexto interno, externo y del proceso. • Implementar el plan de contingencia, documentarlo y analizar la conveniencia de actualizar el mapa de riesgos. • Determinar la efectividad de los controles, confirmando si la ocurrencia del evento se dio por la falta de aplicación de estos o la necesidad de planificar otros. |
| | Segunda línea | OAPII | <p>Acciones frente al reporte de un riesgo materializado:</p> <ul style="list-style-type: none"> • Revisar la información reportada en el sistema de información Gina / Módulo de Riesgos |

D102PR01G01PL03
Versión:01
Fecha: 5/07/2024

| TIPO DE RIESGO | LÍNEA DE DEFENSA | CONDUCTO REGULAR | ACTIVIDADES |
|---|----------------------|---|--|
| | | | <ul style="list-style-type: none"> Asesorar y acompañar a la primera línea de defensa en la revisión o actualización del mapa de riesgos, en particular, las causas, riesgos y controles. Revisar los Planes de tratamiento formulados para cada uno de los riesgos materializados con el fin de tomar medidas para evitar su repetición y lograr el cumplimiento de los objetivos. <p>En los casos de materialización de riesgos de Gestión detectados por la Segunda Línea de defensa, se debe comunicar 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, confirmando que se tomaron decisiones respecto al mapa de riesgos.</p> |
| Riesgos de Corrupción y Fiscales | Primera línea | Jefes de área o Líder del proceso y su equipo de trabajo | <ul style="list-style-type: none"> Implementar el plan de contingencia, documentarlo y reportar en el Sistema de Información GINA el evento o materialización del riesgo con sus evidencias. Informar a la OAPII como segunda línea de defensa, el evento o materialización del riesgo. Atender la situación a través de correcciones y/o haciendo frente las posibles consecuencias. Revisar el mapa de riesgos de corrupción y/o fiscal o integridad pública, en particular, las causas, riesgos y controles existentes y los planes de tratamiento. Revisar el contexto interno, externo y del proceso. Análisis de la materialización con sus causas en mesa de trabajo con la OAPII y la Oficina de Control Interno (esta última de ser necesario). Determinar la efectividad de los controles, confirmando si la ocurrencia del evento se dio por la falta de aplicación de estos o la necesidad de planificar otros. |
| | Segunda línea | OAPII | <p>Acciones frente al reporte de un riesgo materializado:</p> <ul style="list-style-type: none"> Revisar la información reportada en el formulario de materialización de riesgos. Asesorar y acompañar a la primera línea de defensa en la revisión o actualización del mapa de riesgos, en particular, las causas, riesgos y controles. Revisar los Planes de tratamiento formulados para cada uno de los riesgos materializados con el fin de tomar medidas para evitar su repetición y lograr el cumplimiento de los objetivos. <p>En los casos de materialización de riesgos de corrupción o riesgo a la integridad pública o fiscal detectados por la Segunda Línea de defensa, se debe:</p> <ul style="list-style-type: none"> Confirmar si el reporte obedece en realidad a un riesgo de corrupción o riesgo a la integridad pública, evitando posibles diferencias de criterios entorno a la materialización y su implicación disciplinaria. 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. |
| | Tercera línea | OCI | <p>Acciones frente a la posible materialización de un riesgo de corrupción o riesgo a la integridad pública:</p> <ul style="list-style-type: none"> Asesorar a la primera línea de defensa en la revisión o actualización del mapa de riesgos, en particular, las causas, riesgos y controles. Verificar que se tomaron las decisiones correspondientes a la materialización y que estas sean proporcionales a su magnitud. <p>Acciones en caso de identificación de la materialización por la tercera línea de defensa:</p> <ul style="list-style-type: none"> Se deberá convocar al Comité de Coordinación del Sistema de Control Interno. Informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. <p>Es de indicar que, para la gestión de riesgos fiscales, es un deber expreso del Jefe de Control Interno reportar aquellos hechos u operaciones, actos, contratos, programas, proyectos o procesos en ejecución, en donde, en el ejercicio de sus funciones, evidencien un riesgo consolidado o en proceso de consolidación, de</p> |

| TIPO DE RIESGO | LÍNEA DE DEFENSA | CONDUCTO REGULAR | ACTIVIDADES |
|--|------------------|--|---|
| | | | afectación o pérdida de los recursos públicos y/o de bienes o intereses patrimoniales de naturaleza pública. Lo anterior a través del Sistema de Alertas del Control Interno – SACI – de la Contraloría General de la República |
| Riesgos de seguridad de la información | Primera línea | Jefes de área o Líder del proceso y su equipo de trabajo | <ul style="list-style-type: none"> Implementar el plan de contingencia, documentarlo y reportar en el Sistema de Información GINA el evento o materialización del riesgo con sus evidencias Informar a la OAPII como segunda línea de defensa, el evento o materialización del riesgo. Análisis de la materialización con sus causas en mesa de trabajo con la OAPII – OTSI y el líder del proceso donde se materializó el riesgo, de acuerdo con lo reportado en GINA Atender la situación a través de correcciones y/o haciendo frente a las posibles consecuencias. Revisar el mapa de riesgos de seguridad de la información, en particular, las causas, riesgos y controles existentes y los planes de manejo (tratamiento). Revisar el contexto interno, externo y del proceso. Implementar el plan de contingencia, documentarlo y analizar la conveniencia de actualizar el mapa de riesgos. Determinar la efectividad de los controles, confirmando si la ocurrencia del evento se dio por la falta de aplicación de estos o la necesidad de planificar otros. |
| | Segunda línea | OTSI | <p>Acciones frente al reporte de un riesgo materializado:</p> <ul style="list-style-type: none"> Revisar la información reportada en el Sistema de Información GINA Asesorar y acompañar a la primera línea de defensa en la revisión o actualización del mapa de riesgos, en particular, las causas, riesgos y controles. Revisar los Planes de tratamiento formulados para cada uno de los riesgos materializados con el fin de tomar medidas para evitar su repetición y lograr el cumplimiento de los objetivos. |

Fuente: OAPII

16.3 Periodicidad del monitoreo y seguimiento al mapa de riesgos

El monitoreo a la ejecución de los controles y de las acciones del plan de manejo (tratamiento) está a cargo de la primera línea de defensa y el seguimiento. El seguimiento del mapa de riesgos institucional está a cargo de la segunda y tercera línea de defensa, teniendo en cuenta la siguiente tabla:

Tabla 22 Monitoreo y Seguimiento Líneas de Defensa

| Línea de defensa | Riesgos | Vigencia | | | | | | | | | | | |
|------------------------|--|--|-----|-----|---|-----|-----|---|-----|-----|--|-----|-----|
| | | Ene | Feb | Mar | Abr | May | Jun | Jul | Ago | Sep | Oct | Nov | Dic |
| 1ra línea | Todos los tipos de riesgo | Monitoreo Permanente Depende de la periodicidad de la ejecución de los controles | | | | | | | | | | | |
| 2da línea | Riesgos de Gestión Fiscales Seguridad de la Información TI | 1er seguimiento: Con corte al 31 de marzo. La OAPII elaborará el informe de seguimiento durante el siguiente mes después de la fecha de corte del monitoreo | | | 2do seguimiento: Con corte al 30 de junio. La OAPII elaborará el informe de seguimiento durante el siguiente mes después de la fecha de corte del monitoreo | | | 3er seguimiento: Con corte al 30 de septiembre. La OAPII elaborará el informe de seguimiento durante el siguiente mes después de la fecha de corte del monitoreo | | | 4to seguimiento: Con corte al 13 de diciembre. La OAPII elaborará el informe de seguimiento las dos siguientes semanas después de la fecha de corte. | | |
| | Riesgos de Corrupción o a la integridad pública | 1er seguimiento: Con corte al 30 de abril. La OAPII elaborará el informe de seguimiento durante el siguiente mes después de la fecha de corte del monitoreo | | | 2do seguimiento: Con corte al 31 de agosto. La OAPII elaborará el informe de seguimiento durante el siguiente mes después de la fecha de corte del monitoreo | | | 3er seguimiento: Con corte al 31 de diciembre. La OAPII elaborará el informe de seguimiento durante el siguiente mes después de la fecha de corte del monitoreo | | | Este informe dará cuenta de la gestión de prácticas efectivas en la gestión del riesgo, el cumplimiento de las orientaciones metodológicas que deben tenerse en cuenta al momento de reportar la aplicación de controles, acciones de manejo y planes de contingencia, así como, un análisis en función de la mejora continua del modelo de operación, señalando los aspectos que se deben revisar por parte de la primera línea de defensa. | | |
| 3ra línea ⁵ | | 1er seguimiento: Con corte al 30 de abril. En esa medida, la publicación del informe por parte | | | 2do seguimiento: Con corte al 31 de agosto. La publicación del informe por parte de la OCI deberá | | | 3er seguimiento: Con corte al 31 de diciembre. La publicación del informe por parte de la OCI deberá | | | | | |

⁵ De acuerdo con Ley 1474 de 2011 los riesgos de corrupción hacen parte del Plan Anticorrupción y de Atención al Ciudadano (ahora Programa de Transparencia y Ética Pública). El seguimiento a los riesgos corrupción se encuentra definido en el numeral 5. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción teniendo ítem Seguimiento de riesgos de corrupción de la Guía para la administración del riesgo y el diseño de controles en Entidades Públicas versión 6.

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 36 de 41 |

| Línea de defensa | Riesgos | Vigencia | | | | | | | | | | | |
|------------------|---------|---|-----|-----|-----|--|-----|-----|-----|---|-----|-----|-----|
| | | Ene | Feb | Mar | Abr | May | Jun | Jul | Ago | Sep | Oct | Nov | Dic |
| | | de la OCI deberá surtirse en el mes siguiente a la emisión del informe de la segunda línea, es decir en el mes de junio | | | | surtirse en el mes siguiente a la emisión del informe de la segunda línea, es decir en el mes de octubre | | | | surtirse en el mes siguiente a la emisión del informe de la segunda línea, es decir en el mes de febrero. | | | |
| | | Este informe dará cuenta del estado actual en la gestión del riesgo institucional, desde la estructura de la política de administración del riesgo, sus niveles de implementación y resultados en relación con los eventos o materializaciones que han sido evidenciados, e información esencial para la evaluación de la efectividad de las actividades de control establecidas por la entidad frente a la primera y segunda línea de defensa. | | | | | | | | | | | |

Fuente: OAPII

Nota: La evaluación independiente que realiza la Oficina de Control Interno al estado de la gestión del riesgo institucional debe hacerse a través del Módulo de riesgos del Sistema de Información GINA, registrándose allí las recomendaciones de la segunda y tercera línea de defensa, por lo tanto, no debe circunscribirse exclusivamente a la información que consolida la segunda línea de defensa, en ejercicio de su rol.

17 ACTUALIZACIÓN DE LOS MAPAS DE RIESGOS

El mapa de riesgos es revisado y actualizado como mínimo una vez al año a partir de última fecha de revisión. Adicionalmente se deberá realizar una actualización cuando se presenten las siguientes situaciones:

- Cuando existan cambios a la metodología de riesgos
- Cuando exista un cambio de contexto del proceso y/o del Ministerio
- Cuando a partir de un evento de riesgo o una materialización de este se identifiquen nuevas causas: El análisis y actualización se debe realizar sobre el riesgo en mención.
- Cuando exista un cierre eficaz de acciones del plan de tratamiento (manejo) del riesgo. En el análisis y actualización se debe revisar si las actividades ejecutadas cambian la valoración del riesgo y si se requiere formular o no un nuevo plan de tratamiento.
- Cuando se identifiquen riesgos emergentes y cambiantes
- Cuando existen actualizaciones de los documentos metodológicos y normativos y estos a su vez impactan en los riesgos del proceso

Los riesgos identificados podrán ser actualizados de forma individual, cuando así se requiera, tomando como insumos las necesidades de ajuste identificadas en auditorías internas, revisión por la dirección, auditorías externas o resultado de las acciones de seguimiento y autocontrol ejecutadas por los líderes y responsables de proceso. Así mismo, se deben considerar los resultados de los informes de seguimiento (segunda y tercera línea de defensa), pueden viabilizar la necesidad de hacer ajustes a los mapas de riesgos, incluyendo algunas retroalimentaciones específicas relacionadas a la identificación del riesgo, planificación de tratamientos y controles existentes.

Por lo anterior, la actualización o ajuste estará a cargo de los líderes y responsables de procesos (primera línea de defensa), quienes, con el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional, y la información suministrada analizarán la conveniencia de adoptar estos cambios, los cuales están a discrecionalidad de los procesos en su rol de primera línea de defensa.

La actualización de un riesgo no modifica el código de su identificación. El historial del cambios se conservará en el Sistema de Información GINA.

18 COMUNICACIÓN Y CONSULTA

Teniendo en cuenta que la comunicación y consulta con las partes involucradas, tanto internas como externas, debe tener lugar durante todas las etapas del proceso para la gestión del riesgo y las oportunidades, el Ministerio determina las siguientes actividades:

- La Alta Dirección establecerá y actualizará la Política de Gestión de Riesgos, asegurando su socialización en todos los niveles de la Entidad a través de los Comités Estratégicos y de Gestión, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.
- El mapa de Riesgos deberá ser divulgado y estará cargado en el sistema de información GINA / Módulo de Riesgos para consulta de la comunidad del Ministerio. A partir de esto, los colaboradores podrán revisar y retroalimentar en términos de aportar su conocimiento en la identificación, análisis y valoración del riesgo, así como en la ejecución de las acciones definidas para el tratamiento de los riesgos.

D102PR01G01PL03
Versión:01
Fecha: 5/07/2024

- El líder del proceso en su responsabilidad como primera línea de defensa, debe divulgar⁶ los riesgos identificados junto con los controles y las acciones para abordar riesgos a su grupo de trabajo; con la finalidad de generar conciencia y conocimiento de los responsables con el propósito de que se entiendan las bases sobre las cuales se toman las decisiones y las razones por las cuales se requieren dichas acciones. Esta comunicación es importante para aportar al interior del Ministerio la creación de una cultura en la gestión del riesgo.
- La OAPII y la OCI, impulsarán a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- Las acciones de tratamiento de los riesgos priorizados que involucren partes interesadas o terceros serán dadas a conocer por parte de los líderes y responsables de cada proceso.
- La consolidación del Mapa de Riesgos de Corrupción o riesgos a la integridad pública le corresponde realizarla la OAPII, quien servirá de facilitador en el proceso de Gestión de Riesgos de Corrupción con las dependencias.
- La consulta y divulgación del Mapa de Riesgos de Corrupción o riesgos a la integridad pública a partes interesadas y comunidad en general se realizará a través de su publicación en la página web de la Entidad, en la sección de Transparencia y Acceso a la Información Pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, **a más tardar el 31 de enero de cada año.**
- Los riesgos de seguridad digital deberán ser reportados a las autoridades o instancias respectivas que el gobierno disponga, para lo cual el oficial de seguridad asegurará su monitoreo periódico.

19 RIESGOS DE LAVADO DE ACTIVOS Y EL FINANCIAMIENTO DEL TERRORISMO “LA/FT/FPADM”

El sistema permite establecer las políticas y los procedimientos necesarios para la aplicación de un enfoque basado en riesgo en la supervisión de las organizaciones que tienen la obligación de contar con un Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos, Financiación del Terrorismo y Financiación de la proliferación de armas de destrucción masiva.

El Gobierno Nacional con el ánimo de combatir el LA/FT/FPADM ha expedido a través de diferentes entidades públicas, normatividad a través de la cual se establece directrices y lineamientos para que los sujetos obligados, de acuerdo con el sector económico al que pertenecen, adopten sistemas de administración de riesgos de LA/FT/FPADM.

Dado lo anterior podemos encontrar diferentes lineamientos como lo son: el “SAGRILAF” de la Superintendencia de Sociedades, el “SIPLAF” de la Superintendencia de Transporte, el “SIPLAF” de la Superintendencia de Notariado y Registro, el “SIPLA” de la DIAN, el “SARLAF” de la Superintendencia de Economía Solidaria, el “SARLAF” de la Superintendencia de Salud, el “SIPLAF” de Coljuegos, el “SARLAF” del Ministerio de Tecnologías de Información y Comunicaciones, entre otras. Adicionalmente, existen entidades que, sin estar obligadas a ello, deciden adoptar sistemas contra el riesgo de LA/FT/FPADM por temas de autorregulación y buenas prácticas, así, dependiendo de la actividad económica que desarrolle, se estará obligado a adoptar alguno de los sistemas de prevención de LA/FT/FPADM definidos por estas entidades con las que se tenga relación. Desde el Ministerio de Ciencia Tecnología e Innovación se acogerán los lineamientos que al respecto le sean exigidos por los actores con los que opera, así mismo, con base en la normatividad vigente, dará orientaciones sobre los aspectos que se deben tener en cuenta en los procesos contractuales para el cumplimiento de la normatividad aplicable en la materia.

20 GESTIÓN DE LOS RIESGOS DEL SISTEMA DE SEGURIDAD Y SALUD EN EL TRABAJO

La identificación y gestión de los Riesgos del Sistema de Seguridad y Salud en el Trabajo, se realiza mediante la aplicación del procedimiento de “Identificación de peligros, valoración de riesgos y determinación de controles” (A201PR07), a través del cual se identifican los peligros y valorar los riesgos para las operaciones y actividades que generen situaciones adversas que puedan poner en riesgo la salud y seguridad de los servidores públicos, contratistas y visitantes del Ministerio, estableciendo los controles para prevenir accidentes de trabajo, enfermedades laborales y pérdidas materiales.

Para el registro de los riesgos identificados se utiliza la “Matriz de Identificación de Peligros y Valoración de Riesgos” (A201PR07AN01).

21 GESTIÓN DE LOS RIESGOS EN LOS PROCESOS DE CONTRATACIÓN

Atendiendo los lineamientos establecidos en el “Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación”, de Colombia Compra Eficiente, y en el “Manual de Contratación” (A206MO1), para la administración del riesgo en los procesos de contratación, los responsables de la elaboración de los estudios previos, junto con el grupo interdisciplinario responsable de la parte técnica, financiera y jurídica del proyecto deberán atender los siguientes pasos:

⁶ Las metodologías de divulgación pueden ser: correos electrónicos, reuniones presenciales o virtuales, material ilustrativo, entre otras de acuerdo con la capacidad de los procesos, la complejidad de sus riesgos, actividades y las herramientas de comunicación disponibles, quedando a discrecionalidad de cada proceso su propia metodología de divulgación, considerando su liderazgo como primera línea de defensa.

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 38 de 41 |

- Establecer el contexto.
- Identificar y clasificar los riesgos.
- Evaluar y calificar los riesgos.
- Asignación y tratamiento de los riesgos.
- Monitorear los riesgos.

Para desarrollar cada uno de los pasos enunciados anteriormente se debe tener en cuenta lo establecido en el “Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación”, publicado en la página web de Colombia Compra Eficiente, en el siguiente enlace: <https://www.colombiacompra.gov.co/manuales-guias-y-pliegos-tipo/manuales-y-guias>

Para la valoración del riesgo se debe consultar el “Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación”, en el enlace: <https://www.colombiacompra.gov.co/manuales-guias-y-pliegos-tipo/manuales-y-guias>

22 RIESGOS RELACIONADOS CON CALIDAD ESTADÍSTICA

El Ministerio en cumplimiento del Plan de Trabajo para la implementación de la Política de Gestión de la Información Estadística del MIPG y teniendo en cuenta los requisitos de la Norma Técnica de la Calidad del Proceso Estadístico NTCPE 1000:2020, emitida por el Departamento Nacional de Estadística y como miembro del Sistema Nacional de Estadística, se encuentra implementando los requisitos de esa norma para las operaciones estadísticas bajo responsabilidad de la entidad, que se encuentran incluidas en Plan Estadístico Nacional.

En el marco del cumplimiento de esta norma técnica, para la gestión de riesgos con relación directa y podrán afectar la calidad de las operaciones cubiertas por el alcance de la NTC PE 1000:2020, aplicara la metodología utilizada para los riesgos de gestión

23 RIESGOS EMERGENTES

Los riesgos emergentes originados a partir de la globalización, las catástrofes naturales, atentados terroristas y acontecimientos inesperados, las crisis financieras, los nuevos entornos regulatorios a nivel internacional, la innovación tecnológica, la creación de nuevos productos y/o metodologías, exigen a las entidades una adecuada y oportuna gestión del riesgo.

Los riesgos emergentes son aquellos considerados como los riesgos que actualmente no existen o que aún no se reconocen, pero que podrían surgir a raíz de cambios en el entorno. Para dichos riesgos, no aplican los mismos criterios mencionados anteriormente, porque su frecuencia y sus consecuencias son desconocidas. No obstante, la experiencia muestra que cuando se materializan tienen un impacto significativo y, por lo tanto, no se pueden ignorar.

Por lo anterior, cuando se presente un riesgo emergente los procesos frente a la gestión que hacen de los riesgos asociados, deberán identificar cuáles son las amenazas que posiblemente se pueden materializar y que aún no se encuentran incluidas en las matrices de riesgos, dado que si este nace de una actividad que no se ha contemplado en la caracterización del proceso, esta información deberá ser actualizada en las diferentes herramientas de gestión con el fin de controlar aquello que no se tiene documentado formalmente.

En caso de que el proceso identifique estos riesgos no documentados, deberán realizar el análisis del tipo de riesgo al que corresponde, para proceder con la respectiva aplicación de criterios de acuerdo con lo señalado en el presente documento.

24 BIBLIOGRAFÍA

- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA -DAFP (2022). Guía para la administración del riesgo y el diseño de controles en Entidades Públicas. Versión 06.
- ICONTEC Internacional. (2018). NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31000. GESTIÓN DE RIESGO
- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA -DAFP (2023). Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces. Versión 3
- Godoy, E (2018). Riesgo reputacional y riesgo competitivo desde una perspectiva multi-stakeholders. Chile. Alfaomega.

25 DOCUMENTOS ASOCIADOS

- A201PR07 Identificación de peligros, valoración de riesgos y determinación de controles
- A201PR07AN01 Matriz de Identificación de Peligros y Valoración de Riesgos
- A206MO1 Manual de Contratación

D102PR01G01PL03
Versión:01
Fecha: 5/07/2024

26 CONTROL DE CAMBIOS

| Versión | Fecha | Numerales | Descripción de la modificación |
|---------|------------|----------------------|--|
| 05 | 29/10/2024 | 8 17 23 9.1 | <ul style="list-style-type: none"> Se realiza ajuste del documento a la plantilla D102PR01G01PL03 Se incluye la codificación de los riesgos en los lineamientos para la gestión de riesgos. Se amplían las situaciones por las cuales se deben actualizar los riesgos. Se incluye el numeral 23 relacionado con riesgos emergentes. Se incluye la referencia a la herramienta de diagnóstico integral como insumo para el análisis de contexto. |
| 06 | 14/03/2025 | 4 6 8 16.3 | <ul style="list-style-type: none"> Se incluyen nuevas definiciones relacionadas con los riesgos LAFT/FPADM y de debida diligencia. Se incluyen los riesgos de Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva en el alcance de la política. En el punto de lineamientos para la gestión del riesgo se incluyeron orientaciones sobre el riesgo reputacional. Se ajusta la tabla 22 de Monitoreo y Seguimiento Líneas de Defensa, precisando las fechas de corte para la realización de los informes de la segunda y tercera línea de defensa. Igualmente, se especifica la herramienta tecnológica que se debe utilizar para dejar trazabilidad del seguimiento y recomendaciones de la segunda y tercera línea. Se complementa la denominación de los riesgos de corrupción en todo el documento con la expresión riesgos a la integridad pública, de acuerdo con los lineamientos de la Secretaría de Transparencia de la Presidencia de la República. |

| Elaboró | Revisó | Aprobó |
|--|---|---|
| Nombre - Cargo / Rol: Erika Julieth Barragan Cabezas / Contratista / Oficina Asesora de Planeación e Innovación Institucional Edna Del Pilar Páez García / Contratista / Oficina Asesora de Planeación e Innovación Institucional | Nombre - Cargo / Rol: Edna Del Pilar Páez García / Contratista / Oficina Asesora de Planeación e Innovación Institucional | Nombre - Cargo / Rol: César Fabián Gómez Vega / Jefe Oficina Asesora de Planeación e Innovación Institucional |

| | | |
|---|--|----------------------------|
|  | GUÍA PARA LA GESTIÓN DEL RIESGO | Código: D102PR03G01 |
| | | Versión: 06 |
| | | Fecha: 14/03/2025 |
| | | Página: 40 de 41 |

ANEXO 1
CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

La Contraloría General de la República, identificó 50 **puntos de riesgo fiscal** e igual número de **circunstancias inmediatas**, así:

| No. | Puntos de Riesgo Fiscal Actividad en la que potencialmente se origina el riesgo fiscal | Circunstancia Inmediata Situación <u>por la que</u> 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 previsible que debieron ser asignados al contratista en la matriz de riesgos previsible 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 |
| 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 |

D102PR01G01PL03
Versión:01
Fecha: 5/07/2024

| No. | Puntos de Riesgo Fiscal Actividad en la que potencialmente se origina el riesgo fiscal | Circunstancia Inmediata Situación <u>por la que</u> se presenta el riesgo |
|------------|--|--|
| 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 |
| 43 | Actas de recibo final a satisfacción firmadas | Suscripción de acta de recibo final con imprecisiones de fondo |
| 43 | 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) |
| 44 | Predios adquiridos | Adquisición de predios sin las especificaciones técnicas requeridas |
| 45 | Pérdida de tenencia de bienes de la entidad | Pérdida de la tenencia de bienes inmuebles de la Entidad |
| 46 | 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 |
| 47 | Pago de subsidios, transferencias o beneficios a particulares | Pago de subsidio u otros beneficios a personas fallecidas |
| 48 | 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 |
| 49 | Pago de subsidios, transferencias o beneficios a particulares | Pago de subsidios por encima del beneficio otorgado |
| 50 | Deudas a favor de la entidad | Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial |