Comercio,
Industria y Turismo

POLÍTICA Y METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

DE-DR-001

Direccionamiento Estratégico
Noviembre de 2024

TABLA DE CONTENIDO

TÍTULO I. ASPECTOS GENERALES

1. OBJETIVO

Establecer los lineamientos y criterios que orienten al Ministerio de Comercio, Industria y Turismo (MinCIT) en la correcta identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos, a los que se enfrenta la entidad y que puedan impactar el cumplimiento de los objetivos institucionales en el marco de los procesos, planes y proyectos, así como orientar en las acciones que conduzcan a disminuir los efectos de la materialización de los riesgos.

2. ALCANCE

Esta política aplica desde el análisis del Marco Estratégico del Ministerio y de los Objetivos de cada proceso, siguiendo con la identificación, valoración (análisis y evaluación), tratamiento (planificación y definición de acciones de mejora), hasta el monitoreo y seguimiento de los riesgos institucionales.

3. RESPONSABLES

Las responsabilidades para la administración del riesgo se definieron con base en las líneas de defensa[1], se encuentran descritas en el Anexo 1 del presente documento.

4. DEFINICIONES

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que tengan valor para la organización y que sean utilizados para operar en el entorno digital.
- **Administración del Riesgo:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de estos de forma que se apoye el cumplimiento de los objetivos de la entidad.
- **Amenazas:** Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización NTC-ISO/IEC 27000:2017
- **Análisis de Riesgos:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo
- **Análisis del Riesgo:** Proceso que permite comprender la naturaleza del riesgo y determinar el nivel del riesgo NTC-ISO/IEC 27000:2017
- **Apetito de Riesgo**: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito puede ser diferente para los distintos tipos de riesgo que la entidad debe o desea gestionar.
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

  a) *Bien de uso público:* aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.

  b) *Bienes fiscales:* aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo

[1] Las responsabilidades para la administración del riesgo se definieron con base en las líneas de defensa descritas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, anexo 7 criterios diferenciales.

de su misión y utilizados para sus actividades. Ejemplos: 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 la alta dirección considera que no sea 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, correspondiente a las razones por las cuales se puede presentar el riesgo.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.[2]
- **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.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.[3]
- **Evaluación del Riesgo:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo y su magnitud o ambos son aceptables o tolerables. NTC-ISO 31000:2011
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Gestión del Riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)4" . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.
- **Identificación del riesgo:** Proceso de análisis para encontrar una potencial desviación de los objetivos.
- **Impacto:** Resultado de un evento expresado cualitativa o cuantitativamente, como por ejemplo una pérdida, lesión, desventaja o ganancia.

[2] ISO / IEC 27000.2018 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1.
[3] ISO / IEC 27000.2018 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1

- **Integridad:** Propiedad de exactitud y completitud.[4]
- **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.
- **Mapa de Calor:** Plano en el que se presentan simultáneamente las escalas de medición de impacto y de probabilidad, y que, como producto de su combinación, mediante colorimetría representa la importancia (nivel de severidad o criticidad) del riesgo.
- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Materialización del Riesgo:** Ocurrencia o desarrollo del riesgo
- **Nivel de riesgo**: Es el valor que se determina a parir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional del alcanzar los objetivos.
- **Objetivo de proceso**: Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción
- **Oportunidad:** Eventos que permiten alcanzar un resultado esperado o aumentar los efectos deseables.
- **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Política de Administración del Riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **Probabilidad:** Se entiende como 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.
- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Riesgo:** Efecto que causa sobre los objetivos de las entidades, debido a eventos potenciales. **Nota:** Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, falla o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo Fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial2. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).
- **Riesgo de Fraude:** Posibilidad de que la Entidad incurra en una pérdida financiera o de otro tipo cuando una persona (que puede ser empleado, un cliente, o una persona vinculada a la Entidad) que actúa individualmente o en colusión, obtiene una ventaja o beneficio injusto en forma deshonesta o engañosa.
- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre

[4] ISO / IEC 27000.2018 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1

el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riego inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Riesgos de Seguridad y Privacidad de la Información:** posibilidad potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. NTC-ISP 27005:2009 **Nota:** Se mide en términos de una combinación de la probabilidad de que sucede un evento y sus consecuencias. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000:2018).
- **Tolerancia del riesgo**: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Tratamiento del riesgo:** Proceso para modificar el riesgo.
- **Valoración del riesgo:** Proceso general de análisis del riesgo y evaluación del riesgo.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. CONDICIONES GENERALES

En el presente documento se establecen los siguientes parámetros:

- Los riesgos en la seguridad de la información se acogen al presente documento.
- Los riesgos del Sistema de Gestión Ambiental se acogen al presente documento.
- Los riesgos en materia de seguridad y salud en el trabajo (ocupacionales) dando cumplimiento al sistema de gestión de seguridad y salud en trabajo se identifican e implementan de acuerdo con lo establecido en el procedimiento **TH-PR-030 Identificación de peligros y valoración de riesgos.**
- Los riesgos de gestión en materia de contratación se acogen a las Políticas de Colombia Compra Eficiente. Las responsabilidades para la administración del riesgo se definen con base en las líneas de defensa.
- El Contexto de la Organización (cuestiones internas y externas) se define de acuerdo con lo establecido en el procedimiento **DE-PR-014 Formulación y Seguimiento de la Planeación Estratégica Sectorial-PES**.

6. COMUNICACIÓN Y DIVULGACIÓN

La Política y Metodología para la Administración de Riesgos busca crear conciencia en todos los servidores públicos del Ministerio de Comercio, Industria y Turismo, en los distintos niveles y vinculaciones, sobre la importancia de la gestión preventiva y el autocontrol en la ejecución de las actividades y se desarrolla en dos niveles, en los cuales se adelantan acciones o estrategias de comunicación y divulgación según su propósito:

- **A nivel institucional**: Comprende la divulgación y socialización de la Política y Metodología de Administración del Riesgo y el Mapa de Riesgos, la cual estará a cargo de la Oficina Asesora de Planeación Sectorial con el apoyo del Grupo de Comunicaciones. Esta estrategia incluye la publicación en la página web de la entidad, del Mapa de Riesgos de Corrupción y el resultado de los seguimientos.

  Así mismo, dentro de la estructura organizacional formalmente establecida encuentra el Grupo de Comunicaciones con enfoque interno y externo. A nivel interno, garantizan un adecuado flujo de la información a todos los niveles de la organización, mediante el uso de

herramientas tecnológicas (como la Intranet, el correo institucional, la plataforma corporativa Office 365 que incorpora en su suit de aplicaciones a TEAMS como medio virtual de comunicación en línea); así como con la estructura de enlaces en cada dependencia, para el despliegue de la información generada por cualquier medio, y a nivel externo validando los responsables y medios empleados para comunicar información que pueda comprometer de manera equivocada al Ministerio.

- **A nivel de procesos**: Comprende la divulgación de los Mapas de Riesgos por Proceso al interior de los respectivos equipos de trabajo, está a cargo de los responsables de cada Proceso con el apoyo de los gestores de calidad.

7. MARCO CONCEPTUAL PARA NIVELES DE ACEPTACIÓN DEL RIESGO:

La entidad ha definido los niveles de aceptación teniendo en cuenta las siguientes fórmulas:

- **Nivel de riesgo**

Riesgo inherente = Probabilidad inherente vs Impacto inherente

Riesgo Residual = Probabilidad inherente – (Probabilidad Inherente * Control)vs Impacto inherente – (Impacto Inherente * Control)

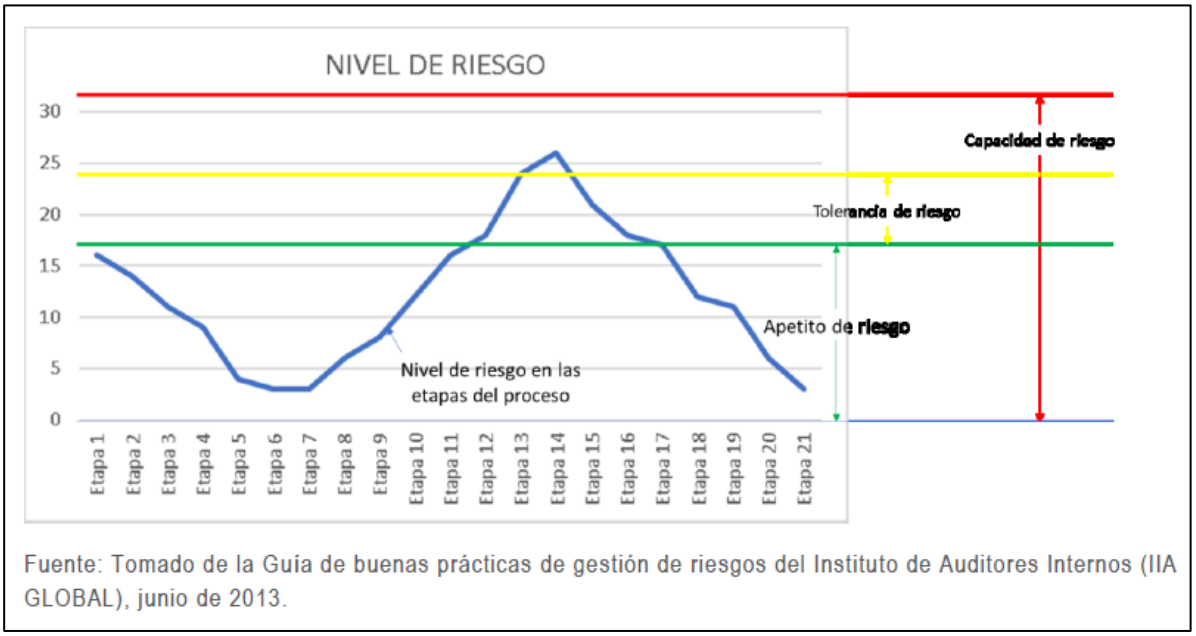
Teniendo en cuenta el apetito, la tolerancia y la capacidad del riesgo, para el Ministerio los niveles de aceptación del riesgo residual son:

	UBICACIÓN EN EL MAPA DE CALOR (Riesgo Residual)	NIVELES DE ACEPTACIÓN	FÓRMULA	ACCIÓN A TOMAR
GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN	Bajo	Apetito del riesgo	# riesgos bajos / Total riesgos	Riesgos aceptados
	Moderado	Tolerancia del riesgo	# riesgos moderados y altos / Total riesgos	Riesgo tolerado sin plan de acción (acciones para abordar riesgos)
	Alto			Riesgo tolerado con plan de acción (acciones para abordar riesgos)
	Extremo	Capacidad del riesgo	# riesgos extremos / Total riesgos	Riesgo soportado con acciones correctivas
FISCALES	Bajo	**Apetito al riesgo**	# riesgos bajos / Total riesgos	Riesgo tolerado sin plan de acción (acciones para abordar riesgos
	Moderado		# riesgos moderados / Total riesgos	Riesgo tolerado sin plan de acción (acciones para abordar riesgos

	Alto	**Tolerancia del riesgo**	# riesgos altos / Total riesgos	Riesgo tolerado con plan de acción (acciones para abordar riesgos)
	Extremo	**Capacidad de riesgo**	# riesgos extremos / Total riesgos	Riesgo soportado con acciones correctivas
CORRUPCIÓN	**Moderado**	**Apetito al riesgo**	# riesgos moderados / Total riesgos	Riesgo tolerado sin plan de acción (acciones para abordar riesgos)
	Alto	**Tolerancia del riesgo**	# riesgos altos / Total riesgos	Riesgo tolerado con plan de acción (acciones para abordar riesgos)
	Extremo	**Capacidad de riesgo**	# riesgos extremos / Total riesgos	Riesgo soportado con acciones correctivas

Tabla 1. Clasificación de Niveles de Aceptación

Estos conceptos se relacionan gráficamente así:



Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

Figura 1: Definiciones de apetito, tolerancia y capacidad de riesgo[5].

[5] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022

TITULO II. IDENTIFICACIÓN DEL RIESGO

1. CONOCIMIENTO Y ANÁLISIS DE LA ENTIDAD:

Antes de iniciar con la metodología para administrar los riesgos es necesario comprender el contexto general del Ministerio (cuestiones internas y externas) y establecer el Marco Estratégico el cual se define para el Ministerio con base en los lineamientos del Plan nacional de Desarrollo.

El Marco Estratégico del Ministerio de Comercio, Industria y Turismo parte de un análisis de contexto que permite reconocer en dónde se encuentra la entidad al revisar y establecer su direccionamiento para el siguiente periodo de gobierno. Este contexto se compone del **contexto externo** (factores: políticos, económicos, financieros, sociales, culturales, tecnológicos, ambientales, legales y reglamentarios), **contexto interno** (misión, visión, estructura organizacional, funciones y responsabilidades, políticas, planeación institucional, objetivos y estrategias implementadas, recursos económicos, personas, procesos, sistemas, tecnología, información, cultura organizacional y relaciones con las partes involucradas) y **contexto del proceso** (objetivo y alcance del proceso, interrelación con otros procesos, planes, programas o proyectos asociados y activos de seguridad y privacidad de la información del proceso) y como resultado se definen los ejes estratégicos y el despliegue de estos. (Ver **Marco Estratégico MinCIT**.)

El conocimiento del contexto facilita la identificación de riesgos y oportunidades para el cumplimiento de los objetivos estratégicos.

2. CLASIFICACIÓN DEL RIESGO

Los riesgos se clasifican así:

TIPO	CLASIFICACIÓN	DESCRIPCIÓN
RIESGOS DE GESTIÓN	**EJECUCIÓN Y ADMINISTRACIÓN DE PROCESOS**	Pérdidas derivadas de errores en la ejecución y administración de procesos.
	FRAUDE EXTERNO	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
	FRAUDE INTERNO	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
	FALLAS TECNOLÓGICAS	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
	RELACIONES LABORALES	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
	USUARIOS, PRODUCTOS Y PRÁCTICAS	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

TIPO	CLASIFICACIÓN	DESCRIPCIÓN
	DAÑOS A ACTIVOS FIJOS/ EVENTOS EXTERNOS	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
	LEGALES	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad debido a su incumplimiento o desacato a la normativa vigente.
RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Pérdida de confidencialidad – privacidad, Integridad y/o disponibilidad de los activos de información institucionales por la combinación de amenazas y vulnerabilidades en el entorno físico y/o digital que pueden afectar a las personas, el logro de objetivos económicos, sociales o ambientales, o la relación con otros sectores a nivel nacional
RIESGOS DE CORRUPCIÓN		Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
RIESGO FISCAL		Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Tabla 2. Clasificación de Riesgos[6]

3. DESCRIPCIÓN DEL RIESGO:

Los **Riesgos se identifican a partir del Marco Estratégico del MinCIT**, o el documento que establezca el direccionamiento estratégico, que estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los **objetivos estratégicos o del proceso**.

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 las personas ajenas a él. A continuación, se relaciona la estructura que facilita su redacción y claridad.

Desglosando la estructura tenemos:

Impacto: Aquí definimos el ¿Qué puede pasar?, los factores de impacto a los que puede estar expuesta la entidad

- **Causa inmediata:** nos responde al ¿Cómo puede pasar?, son las situaciones más evidentes por las cuales se puede materializar el riesgo.

- **Causa raíz:** nos da respuesta al ¿Por qué puede pasar? Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas. Esta es la base para la definición de los controles.

[6] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

El esquema para la redacción del riesgo es:

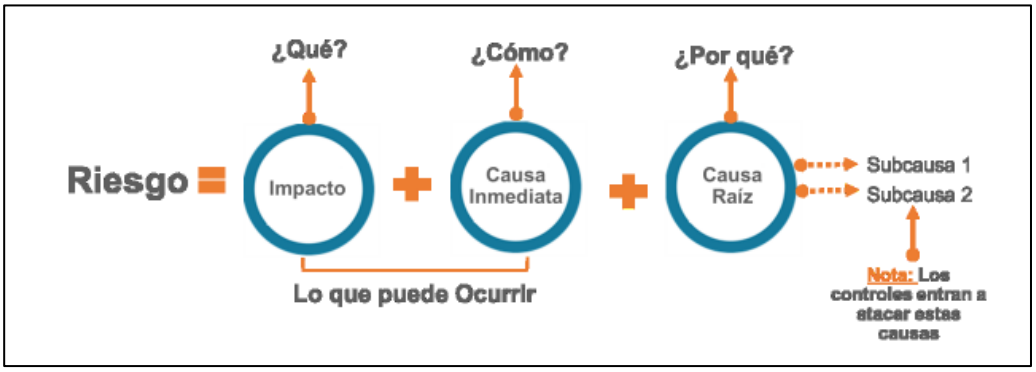


Figura 2. Estructura propuesta para la redacción del riesgo y ejemplo[7]

Ejemplo:

Incumplimiento de los requisitos legales para la liquidación y terminación de un contrato

Recomendaciones:

- No describir como omisiones ni desviaciones de control.
  Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- No describir causas como riesgos.
  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- No describir riesgos como la negación de un control.
  Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.
- No existen riesgos transversales, lo que pueden existir son causa transversales.
  Ejemplo: pérdida de expedientes.
- Evitar 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 en el lector o escucha la imagen del evento como si ya estuviera sucediendo.
- Pregúntese si el riesgo identificado está relacionado directamente con las características del objetivo. Si la respuesta es "no", lo descrito puede ser la causa o la consecuencia del riesgo.

3.1 Riesgos de Gestión

La redacción final del riesgo estará dada en los términos en que se haya presentado la valoración del impacto, es decir:

[7] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

La posibilidad de afectación se tomará de acuerdo a la mayor valoración que se haya presentado frente a los parámetros de impacto; si el riesgo obtuvo una valoración de impacto económico bajo y una valoración reputacional mayor, la descripción se realizará en términos de afectación reputacional.

3.2 Riesgos de Corrupción

Corresponde al líder de proceso la identificación de escenarios de corrupción, con el fin de implementar los mecanismos de seguimiento y prevención de la corrupción, identificando los elementos de omisión, acción que mediante el uso del poder terminen desviando la gestión de lo público.

Se puede determinar si un riesgo es de corrupción, si se marca con una X en la descripción del riesgo las situaciones señaladas en la siguiente tabla:

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Riesgo de **Corrupción**	X	X	X	X

Tabla 3. Determinación del Riesgo de Corrupción

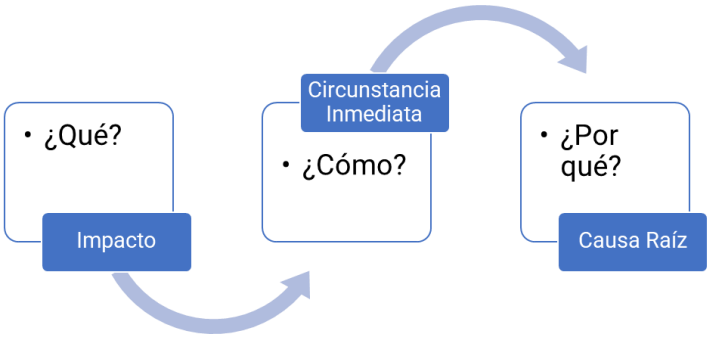
3.3 Riesgos Fiscales

Según lo descrito en la guía para la administración del riesgo y el diseño de controles en entidades públicas, V6, define y describe la composición del riesgo fiscal en sus siguientes elementos:

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.

Es decir que para describir el riesgo se deben tener implícitos los siguientes aspectos:



Ejemplo de redacción del Riesgo Fiscal:

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

3.4 Riesgos de Seguridad y privacidad de la Información

Pérdida de confidencialidad – privacidad, Integridad y/o disponibilidad de los activos de información institucionales por la combinación de amenazas y vulnerabilidades en el entorno físico y/o digital que pueden afectar a las personas, el logro de objetivos económicos, sociales o ambientales, o la relación con otros sectores a nivel nacional.

Corresponde al Líder de Seguridad y Privacidad de la Información y al Líder del Proceso, identificar los activos de información en los que su confidencialidad, integridad o disponibilidad se vean afectadas por causa de amenazas y vulnerabilidades del entorno físico o digital que en la operación puedan materializar el riesgo.

En la identificación de activos de información se aplican la Guía Activos de Información (GTI-DE-001) que orienta sobre los tipos de activos - información, hardware, personas, software, servicios, Intangible e Infraestructura física o Tecnológica – y su documentación en el Inventario de Activos de Información (GTI-FM-015).

Para la gestión y administración de los riesgos, se cuenta con el formato GTI-FM-024: Matriz de Riesgos de Seguridad y Privacidad de la Información.

TITULO III. VALORACIÓN DEL RIESGO

La valoración del riesgo consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de impacto, con el fin de estimar la zona de riesgo inicial o propio de la actividad también llamado *"RIESGO INHERENTE"*.

1. ANÁLISIS DE RIESGO

Consiste en establecer la probabilidad de ocurrencia y el nivel de impacto del riesgo, con el fin de estimar su severidad (RIESGO INHERENTE).

1.1. Determinar la PROBABILIDAD: se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? Está asociada a la exposición al riesgo del proceso o actividad que se está analizando, se trata en este caso de un hecho que no se ha presentado, pero es posible, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, o tratándose de hechos que se han materializado o frente a los cuales se cuenta con un historial de situaciones o eventos asociados al riesgo.

A continuación, se establecen los criterios para definir el nivel de probabilidad, tanto para los riesgos de gestión, fiscales, de corrupción y de seguridad en la información:

NIVEL	FRECUENCIA DE LA ACTIVIDAD	FRECUENCIA DE EVENTOS* Interpretación	PROBABILIDAD
MUY BAJA	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	El evento no ha ocurrido en los últimos **10 años o más**, y las circunstancias que lo harían posible son extremadamente improbables	20%
BAJA	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	El evento no ha ocurrido en los últimos **5 a 10 años**, pero podría materializarse en situaciones específicas	40%
MEDIA	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	El evento se ha presentado **al menos una vez cada 2 a 5 años**. Las condiciones actuales sugieren que podría repetirse bajo circunstancias desfavorables	60%
ALTA	La actividad que conlleva el riesgo se ejecuta de 500	El evento ocurre con frecuencia **cada 6 a**	80%

NIVEL	FRECUENCIA DE LA ACTIVIDAD	FRECUENCIA DE EVENTOS* Interpretación	PROBABILIDAD
	veces al año y máximo 5.000 veces por año.	**12 meses**, asociado a vulnerabilidades conocidas, procesos críticos o alta exposición de actores clave en la gestión.	
MUY ALTA	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año.	El evento ocurre con frecuencia **cada 3 a 6 meses**, evidenciando procesos recurrentemente vulnerables o actores clave implicados con alta probabilidad de recurrencia	100%

Tabla 4. Criterios para definir la frecuencia de la actividad en el nivel de PROBABILIDAD de ocurrencia de los riesgos[8].

*Tomarlo como referencia para análisis de probabilidad en riesgos de corrupción (construcción propia)

- **Nota:** En materia de tecnología (incluye disponibilidad de aplicativos) se tiene en cuenta 1 hora de funcionamiento = 1 vez.

1.2. Determinar el IMPACTO: este se determina para establecer lo que la entidad podría llegar a perder, con el fin de estimar la zona de riesgo en caso de no controlarse (RIESGO INHERENTE). Para definir la tabla de criterios, las variables principales que se tienen en cuenta son impactos económicos y reputacionales, pero pueden adicionarse más variables que permitirán tener más opciones al momento de valorar el riesgo.

En caso de que un riesgo de gestión pueda ser valorado en términos de impacto económico y reputacional, y su calificación se encuentre en distintos niveles, se tomará el nivel de calificación más alto para hallar el riesgo inherente.

Para los riesgos de **Corrupción** se tiene en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos. En este orden de ideas, no se contemplan los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

NIVEL	VALOR IMPACTO / RIESGOS	
	Riesgos de Gestión, Fiscales y de Seguridad y privacidad de la Información	Riesgos de Corrupción
LEVE	20%	N/A
MENOR	40%	

[8] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

NIVEL	VALOR IMPACTO / RIESGOS	
	Riesgos de Gestión, Fiscales y de Seguridad y privacidad de la Información	Riesgos de Corrupción
MODERADO	60%	60%
MAYOR	80%	80%
CATASTRÓFICO	100%	100%

Tabla 5. Criterios para definir el nivel de impacto riesgos de la entidad vs riesgos de corrupción

La calificación del impacto de los **riesgos de Gestión y Fiscales** en la parte económica se estima de acuerdo con el presupuesto de funcionamiento asignado al ministerio, después de realizadas las transferencias a las entidades:

NIVEL	AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL
LEVE	Afectación menor al 1% del presupuesto de funcionamiento del ministerio	El riesgo afecta la imagen de una dirección, coordinación u oficina de la entidad
MENOR %	Entre el 1% y menor al 3% del presupuesto de funcionamiento del ministerio	El riesgo afecta la imagen de un viceministerio, despacho del ministro, o Secretaría general de la entidad,
MODERADO	Entre el 3% y menor al 7% del presupuesto de funcionamiento del ministerio	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
MAYOR 80%	Entre el 7% y menor al 15% del presupuesto de funcionamiento del ministerio	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel del sector administrativo.
CATASTROFICO 100%	Afectación mayor al 15% del presupuesto de funcionamiento del ministerio	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Tabla 6. Criterios para definir el nivel de Impacto en el riego

Para calificar el **impacto de los riesgos de corrupción** se debe responder el siguiente cuestionario:

No.	PREGUNTA: Si el Riesgo de Corrupción se materializa podría:	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Tabla 7. Preguntas para calificar el impacto / consecuencia – RIESGO DE CORRUPCIÓN

De acuerdo con el resultado anterior, el número de preguntas contestadas afirmativamente permitirá ubicar el riesgo según la siguiente tabla y determinar el impacto / consecuencias del riesgo de corrupción:

DESCRIPTOR	CANTIDAD DE PREGUNTAS AFIRMATIVAS	IMPACTO / CONSECUENCIAS CUALITATIVO
CATASTRÓFICO 100%	DOCE a DIECINUEVE preguntas	Genera consecuencias desastrosas para la entidad
MAYOR 80%	SEIS a ONCE preguntas	Genera altas consecuencias sobre la entidad.
MODERADO 60%	UNA a CINCO preguntas(s)	Genera medianas consecuencias sobre la entidad

Tabla 8. Calificación impacto / consecuencia – RIESGO CORRUPCION

Para calificar el impacto de los **Riesgos de Seguridad y privacidad de la Información** se debe tener en cuenta la siguiente tabla:

RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
NIVEL	**CUANTITATIVAS - ECONÓMICA**	**CUALITATIVAS - REPUTACIONAL**
CATASTRÓFICO **100%**	- Afectación mayor o igual al 50% de la población. - Afectación mayor o igual al 50% del presupuesto anual de Tecnologías de la Información para la gestión de seguridad digital. - Afectación muy grave del medio ambiente que requiere de mayor o igual a 3 años de recuperación.	- Afectación muy grave de la integridad de la información debido a la **pérdida de información crítica para la entidad que no se puede recuperar.** - Afectación muy grave de la disponibilidad de la información debido **a la interrupción de las operaciones de la entidad por más de cinco (5) días.** - Afectación muy grave de la confidencialidad **y privacidad** de la información debido **a la fuga de información crítica no autorizada.**
MAYOR **80%**	- Afectación en un valor igual o mayor al 20% e inferior al 50% de la población. - Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto anual de Tecnologías de la Información para la gestión de seguridad digital. - Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	- Afectación grave de la integridad de la información debido a la **pérdida de información crítica para la entidad que se puede recuperar parcialmente.** - Afectación grave de la disponibilidad de la información debido **a la interrupción de las operaciones de la entidad entre dos y tres días.** - Afectación grave de la confidencialidad **y privacidad** de la información debido **a la exposición de información crítica por parte de empleados y/o terceros.**
MODERADO **60%**	- Afectación en un valor igual o mayor al 10% y menor al 20% de la población. - Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto anual de Tecnologías de la Información para la gestión de seguridad digital.	-Afectación moderada de la integridad de la información debido a la **pérdida de información crítica para la entidad o del servicio de aplicación que se puede recuperar de manera inmediata.**

RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
NIVEL	**CUANTITATIVAS - ECONÓMICA**	**CUALITATIVAS - REPUTACIONAL**
	- Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación.	- Afectación moderada de la disponibilidad de la información debido **a la interrupción de las operaciones de la entidad no mayor a 24 horas.** - Afectación moderada de la confidencialidad **y privacidad** de la información debido **a la publicación o entrega de información sensible no anonimizada a terceros.**
MENOR **40%**	-Afectación en un valor igual o mayor al 1% y menor al 10% de la población. -Afectación en un valor igual o mayor al 1% y menor al 10% del presupuesto anual de Tecnologías de la Información para la gestión de seguridad digital. -Afectación leve del medio ambiente requiere de Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	-Afectación menor de la integridad de la información debido a cambios definidos por el proceso para la **recopilación de datos y evaluación de la información.** - Afectación menor de la disponibilidad de la información debido **a la interrupción programada entre 1 y 6 horas de los servicios de aplicación por ajustes a funcionalidades.** - Afectación menor de la confidencialidad **y privacidad** de la información por cambios del entorno de control del proceso**.**
LEVE **20%**	-Afectación en un valor menor al 1% de la población. -Afectación en un valor menor al 1% del presupuesto anual de Tecnologías de la Información para la gestión de seguridad digital. -No hay afectación medioambiental.	-Sin afectación de la integridad de la información gestionada por el proceso. -Sin afectación de la disponibilidad de la información o los servicios de aplicación que soportan el proceso. -Sin afectación de la confidencialidad y privacidad de la información que gestiona por el proceso.

Tabla 9. Criterios para calificar el impacto / consecuencia – RIESGO DE SEGURIDAD DE LA INFORMACION

2. EVALUACIÓN DEL RIESGO – NIVEL DE RIESGO INHERENTE (SEVERIDAD)

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). Para establecer el nivel de riesgo inherente (sin aplicación de controles) y residual (con aplicación de controles) se utilizan los Mapas de Calor, que permiten ubicar el riesgo en la zona de acuerdo con la calificación de la **probabilidad** y el **impacto.**

Para todos los riesgos de **gestión, fiscales y de seguridad de la información**, se definen cuatro zonas de severidad en el mapa de calor como se menciona a continuación:

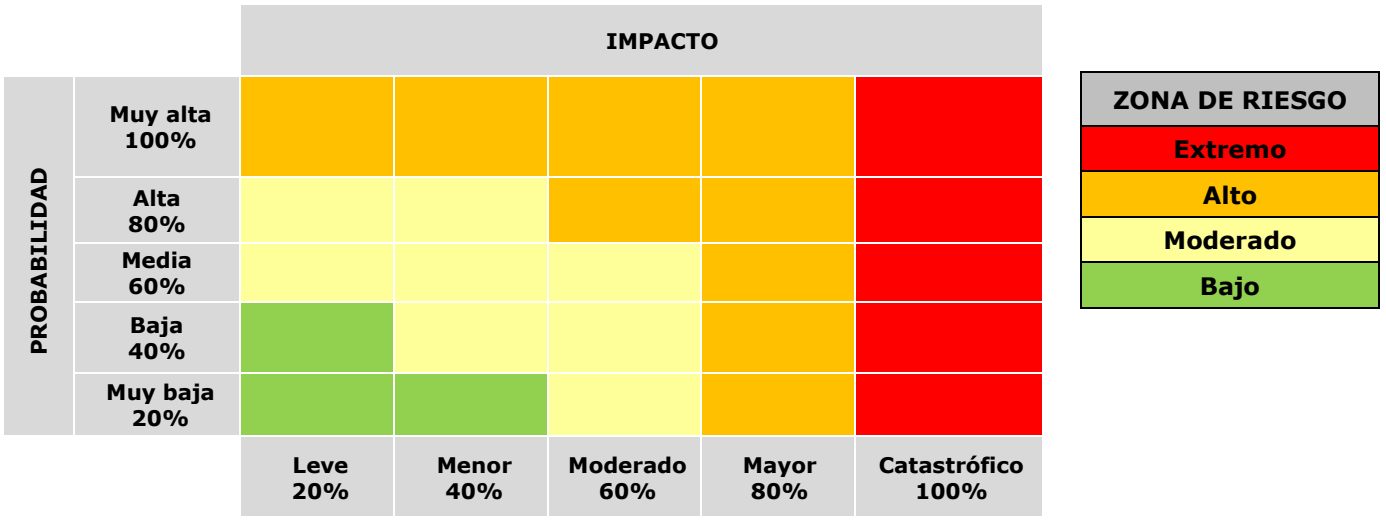
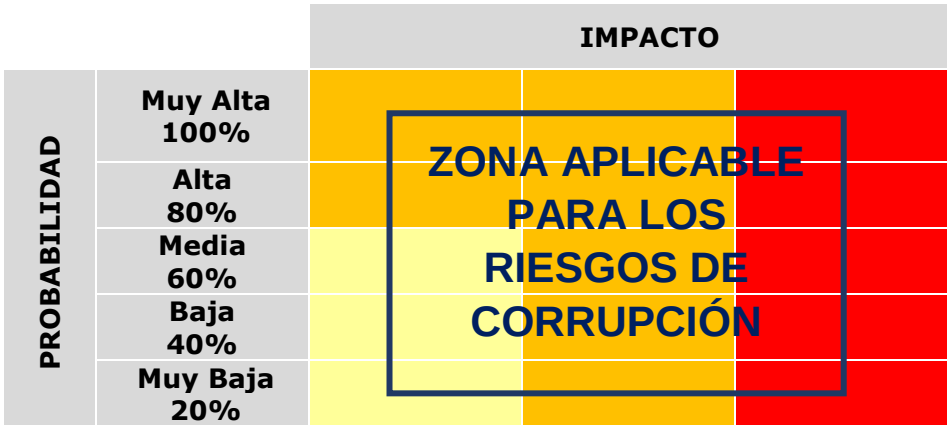


Figura 4. Mapa de Calor Riesgo Inherente[9]

- **Riesgo de Corrupción**



[9] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

Moderado 60%	**Mayor 80%**	**Catastrófico 100%**

Figura 5. Mapa de calor para riesgos de corrupción[10]

3. DISEÑO Y VALORACIÓN DE CONTROLES

Los controles o actividades de control son medidas que permiten reducir o mitigar las causas que hacen que el riesgo se materialice, por eso la importancia en su diseño y evaluación.

3.1Determinación de controles

Con el fin de asegurar la efectividad de los controles se hace necesario, debe contener una estructura en cuanto a descripción, atributos informativos y de eficiencia.

- La descripción debe contener: el responsable de ejecutar el control (cargo del servidor que ejecuta el control; acción (determinada mediante verbos) y complemento (identificar claramente el objeto del control)
- Atributos informativos: deben contener información acerca de si el control está documentado (procedimiento, manuales propios del proceso etc.); la frecuencia de ejecución de la actividad (continua u aleatoria); y la evidencia en cuanto a si se deja un registro del control o no.
- Atributos de eficiencia: corresponden al tipo de control (preventivo, detectivo, correctivo); y su implementación (automático o manual).

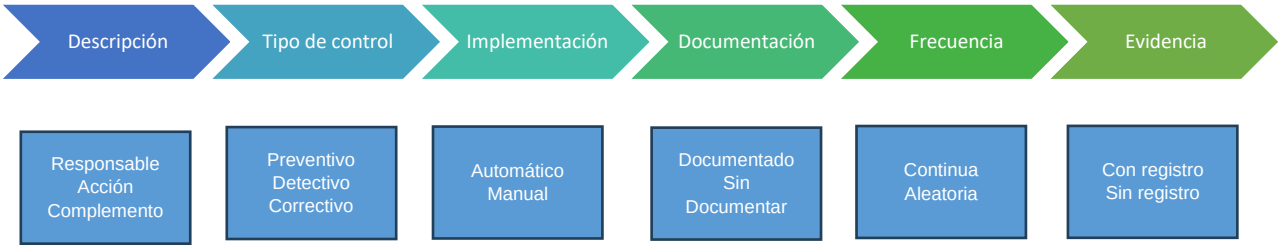


Figura 6. Elementos de un control.

La identificación de los controles se realiza a partir de cada una de las causas raíz que se hayan identificado para cada riesgo, y son los responsables o líderes de los procesos quienes implementan y aseguran el seguimiento de dichos controles con el apoyo de su equipo de trabajo.

Redacción de un control

Es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitiguen las causas que generan la materialización del riesgo. Esto se debe tener en cuenta desde la redacción de este.

Ejemplo:

[10] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

El profesional de Contratación (responsable), verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación (acción), a través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación (complemento).

- **Tipología del Propósito de los Controles**

Se deben seleccionar actividades de **control preventivo, detectivo y correctivo** que por sí solos ayuden a la mitigación las **causas** que originan los riesgos. Para cada causa debe existir un control. Un control puede ser tan eficiente que ayude a mitigar varias causas.

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

CONTROLES PREVENTIVOS	CONTROLES DETECTIVOS	CONTROLES CORRECTIVOS
•Va a las causas del riesgo. Atacan la probabilidad de ocurrencia del riesgo.	•Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad de ocurrencia del riesgo.	•Atacan el impacto frente a la materialización del riesgo.

Figura 7. Tipologías de controles[11]

De acuerdo con la tipología del control es importante considerar:

- **Controles Preventivos:** son accionados antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Controles Detectivos:** son accionados durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reproceso.
- **Controles Correctivos:** son accionados después de que se materializa el riesgo. Estos controles tienen costos implícitos.

De acuerdo con la **forma** como se ejecutan los controles tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

Es importante que para la adecuada mitigación de los riesgos no baste solo con que un control este bien diseñado, el control **debe ejecutarse por parte de los responsables tal como se diseñó.**

3.2 Análisis y evaluación de controles (Atributos) para los Riesgos de Gestión, Fiscales y de seguridad y privacidad de la información

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Los aspectos sin peso son atributos informativos que no tienen incidencia directa en la efectividad del control, sin embargo, permiten darle formalidad a éste.

[11] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

Los aspectos de Tipo e Implementación son atributos que tienen incidencia directa en la efectividad del control, su valoración suma máximo 50% y mínimo 25%.

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 en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	N.A
		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.	N.A
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	N.A
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	N.A
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	N.A
		Sin registro	El control no deja registro de la ejecución del control.	N.A

Tabla 10. Atributos para el diseño de controles[12]

3.3 Análisis y evaluación de controles para los Riesgos de Corrupción

[12] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

La valoración de los controles en los riesgos de corrupción se encuentra ligada a seis variables que denotan tanto el diseño del control, como su ejecución de acuerdo a la siguiente tabla:

CRITERIO DE EVALUACIÓN		ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1. Responsable	1.1 Asignación del responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
			No asignado	0
	1.2 Segregación y autoridad del responsable.	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
			Inadecuado	0
2. Periodicidad		¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
			Inoportuna	0
3. Propósito		¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar, Cotejar, Comparar, Revisar, ¿etc.?	Prevenir	15
			Detectar	10
			No es un control	0
4. Cómo se realiza la actividad de control		¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable
5. Qué pasa con las observaciones o desviaciones		¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
			No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control		¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?	Completa	10
			Incompleta	5
			No existe	0

Resultados de la evaluación del diseño del control

De acuerdo con los pesos asignados a cada una de las variables de diseño y según lo dispuesto en la siguiente tabla se considerará si el diseño del control es FUERTE, MODERADO o DÉBIL.

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
FUERTE	Calificación entre 96 y 100
MODERADO	Calificación entre 86 y 95
DÉBIL	Calificación entre 0 y 85

Resultados de la evaluación de la ejecución del control

De acuerdo con los pesos asignados a cada una de las variables de ejecución y según lo dispuesto en la siguiente tabla se considerará si el diseño del control es FUERTE, MODERADO o DÉBIL.

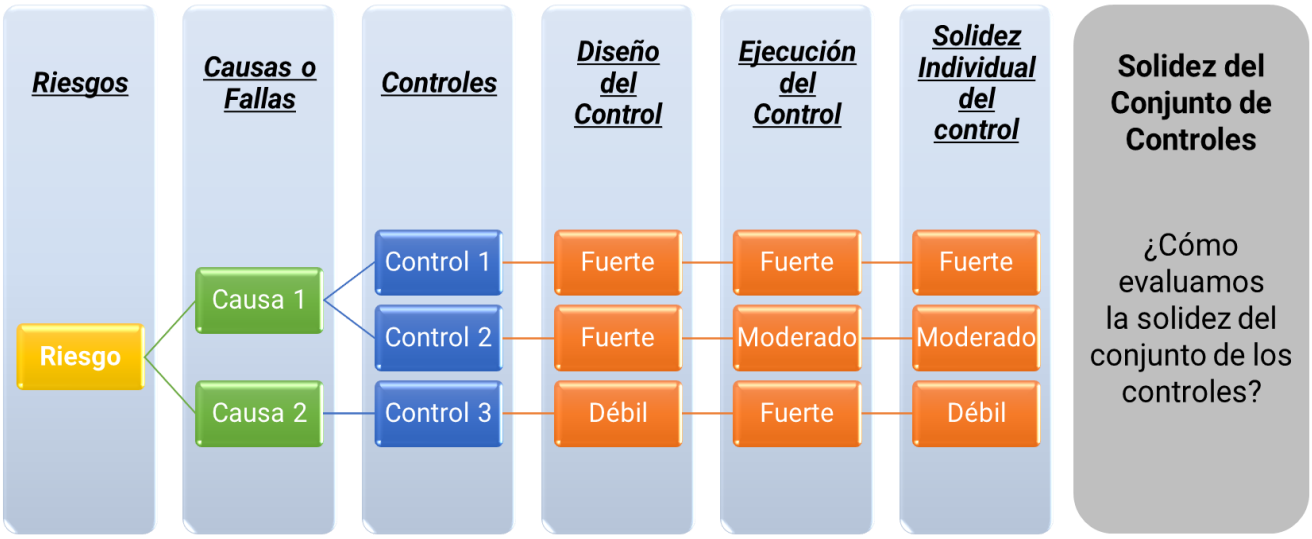
RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO DE LA EJECUCIÓN DEL CONTROL
FUERTE	El control se ejecuta de manera consistente por parte del responsable
MODERADO	El control se ejecuta algunas veces por parte del responsable.
DÉBIL	El control no se ejecuta por parte del responsable.

Análisis y evaluación de los controles para la mitigación de los riesgos

El peso individual de cada control se da tomando como base la respuesta de valoración del diseño y valoración de la ejecución, y se determinara de acuerdo con lo establecido en la siguiente tabla:

PESO INDIVIDUAL DEL DISEÑO DEL CONTROL	*EL CONTROL SE EJECUTA DE MANERA CONSISTENTE POR LOS RESPONSABLES (EJECUCIÓN)	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:100 MODERADO:50 DEBIL: 0	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL SI/NO
FUERTE Calificación entre 96 y 100	Fuerte (siempre se ejecuta)	Fuerte + Fuerte = Fuerte	NO
	Moderado (algunas veces)	Fuerte + Moderado = Moderado	SI
	Débil (no se ejecuta)	Fuerte + Débil = Débil	SI
***MODERADO Calificación entre 86 y 95**	Fuerte (siempre se ejecuta)	Moderado + Fuerte = Moderado	SI
	Moderado (algunas veces)	Moderado + Moderado = Moderado	SI
	Débil (no se ejecuta)	Moderado + Débil = Débil	SI
***DÉBIL Calificación entre 0 y 85**	Fuerte (siempre se ejecuta)	Débil + Fuerte = Débil	SI
	Moderado (algunas veces)	Débil + Moderado = Débil	SI
	Débil (no se ejecuta)	Débil + Débil = Débil	SI

Solidez del conjunto de controles para la adecuada mitigación del riesgo



La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
FUERTE	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
MODERADO	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
DÉBIL	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

4. NIVEL DE RIESGO RESIDUAL

Corresponde al resultado de **aplicar la efectividad de los controles** al riesgo inherente. A continuación, se muestran las fórmulas para la aplicación de controles y establecer el riesgo residual:

Riesgo Residual = Probabilidad inherente – (Probabilidad Inherente * Control)
Impacto inherente – (Impacto Inherente * Control)

Nota:

- En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente (impacto inherente), es importante señalar que no es posible su movimiento en el mapa de calor para el impacto.
- Cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

La solidez del conjunto de controles se define acorde a la tabla 10 por cada riesgo. Con la calificación obtenida se realiza un desplazamiento en el mapa de calor, así: si el control afecta la probabilidad se avanza hacia abajo. Si afecta el impacto se avanza a la izquierda:

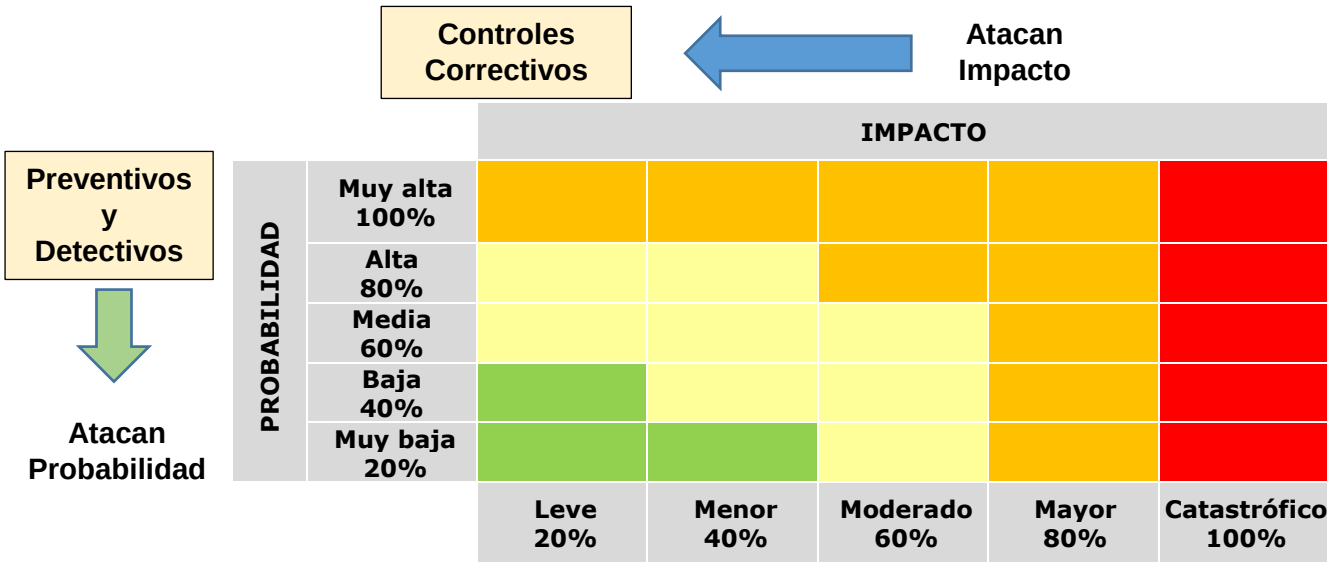


Figura 8. Movimiento en el mapa de calor acorde con el tipo de control riesgo residual[13]

Una vez realizado el análisis y evaluación de los controles se valora nuevamente la probabilidad e impacto/consecuencia del riesgo, determinando si los controles ayudan o no a la disminución probabilidad e impacto del riesgo y se procede a ubicar el **riesgo residual** en el **Mapa de Riesgo Residual.**

5. NIVELES DE ACEPTACIÓN DEL RIESGO RESIDUAL

[13] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022.

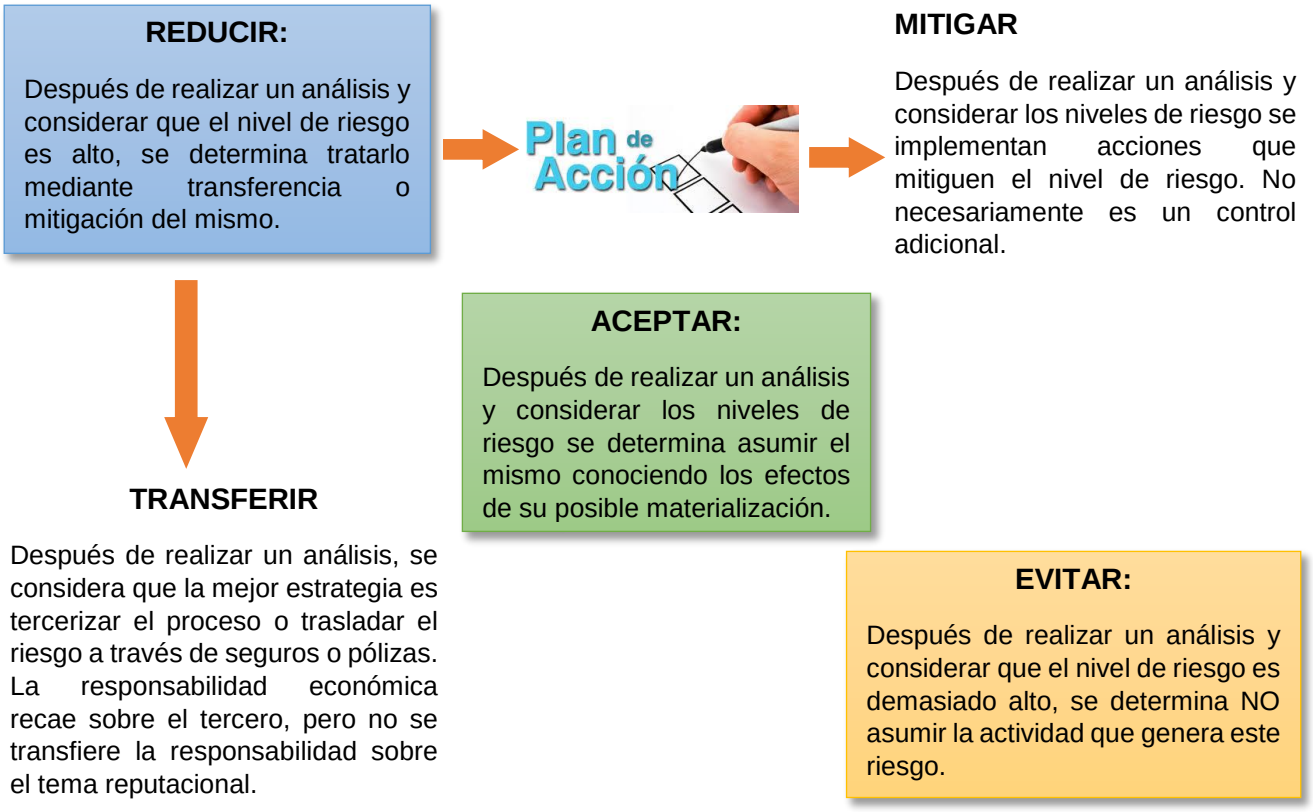


Figura 9. Criterios de aceptación del Riesgo Residual[14].

De acuerdo con la valoración de cada riesgo residual y su ubicación en la zona de riesgo (extremo, alto, moderado, bajo) se establece su opción de manejo. Esto se define a partir del nivel del riesgo residual (con controles), de la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

Dependiendo del valor del riesgo residual, este se puede:

A partir de los criterios RAE (Reducir, Aceptar y Evitar), el Ministerio establece las siguientes acciones para los niveles de aceptación a los riesgos así:

CRITERIOS	ACCIONES
ACEPTAR	Se debe asumir el riesgo y el impacto de su materialización en caso que se presente.
EVITAR	Se debe eliminar, evitar o cambiar la actividad generadora del riesgo.
REDUCIR	Adoptar acciones para abordar riesgos encaminadas a reducir, mitigar o transferir el riesgo, generando un plan de acción a partir de la materialización del riesgo o cuando después de dos (2) monitoreos consecutivos, por lo menos uno de los controles demuestre ineficacia.

[14] Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de Noviembre de 2022

Tabla 11. Acciones para los niveles de aceptación del Riesgo Residual

De acuerdo con la ubicación en la zona del riesgo residual se deben implementar los siguientes niveles de aceptación:

ZONA DE RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESIDUAL		
	Gestión y Seguridad y Privacidad de la Información	**Fiscales**	**Corrupción**
Bajo	**ACEPTAR - EVITAR**	**Ningún** riesgo de corrupción podrá ser aceptado	**Ningún** riesgo de corrupción podrá ser aceptado.
Moderado	**ACEPTAR - EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) - ACEPTAR**	**REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) - EVITAR**	**REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO) - EVITAR**
Alto	**EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)** • Se deben establecer planes de acción según sea el caso, así como el indicador que permita evidenciar la eficacia y efectividad del mismo.	**EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)** Se deben establecer planes de acción según sea el caso, así como el indicador que permita evidenciar la eficacia y efectividad del mismo.	**EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)** • Se deben establecer planes de acción según sea el caso, así como el indicador que permita evidenciar la eficacia y efectividad del mismo.
Extremo	**EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)** • Se deben establecer planes de acción según sea el caso, así como el indicador que permita evidenciar la eficacia y efectividad del mismo	**EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)** Se deben establecer planes de acción según sea el caso, así como el indicador que permita evidenciar la eficacia y efectividad del mismo	**EVITAR - REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)** • Se deben establecer planes de acción según sea el caso, así como el indicador que permita evidenciar la eficacia y efectividad del mismo

Tabla 12. Niveles de aceptación del Riesgo Residual.[15]

[15] Fuente: Elaboración propia Ministerio Comercio, Industria y Turismo.

TÍTULO IV. MONITOREO Y EVALUACIÓN A LOS RIESGOS

En cuanto al esquema de líneas de defensa, el Modelo Integrado de Planeación y Gestión MIPG desarrollado en la dimensión 7 del Modelo estándar de control interno MECI, se define como el eje articulador para la identificación de la responsabilidad frente a la gestión del riesgo y control compartido por los servidores públicos de la entidad

- **Monitoreo línea estratégica**

La Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno como responsable de la línea estratégica adelanta el monitoreo centrado en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad.

- **Monitoreo primera línea de defensa:**

A los servidores del Ministerio en sus diferentes niveles les corresponde implementar la línea de defensa con las medidas de control interno en las operaciones del día a día de la entidad.

Se debe precisar que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles de gerencia operativa, ya que son aplicados por líderes o responsables de proceso. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos.

Los líderes de los procesos en conjunto con sus equipos de trabajo, producto de las revisiones periódicas a los riesgos definidas en el presente documento, y en caso de ser necesario pueden solicitar a la Oficina Asesora de Planeación ajustes a cualquier de las etapas de los riesgos. Así mismo, en caso de materialización de un riesgo se debe informar a la Oficina Asesora de Planeación Sectorial (OAPS), con el fin de solicitar el acompañamiento para la generación del plan de acción.

El monitoreo a los riesgos lo empieza a realizar la primera línea de defensa (responsables de proceso y equipos de trabajo), mediante la revisión del cumplimiento de los objetivos establecidos en el proceso y sus indicadores de desempeño, identificando en caso de que no se estén cumpliendo, las alertas que conlleven a una posible materialización del riesgo en el cumplimiento de los objetivos.

- **Monitoreo segundo línea de defensa:**

La Segunda Línea de Defensa en el Ministerio la integran el Jefe de la Oficina Asesora de Planeación Sectorial, Directores, Secretaría General y Coordinadores de Contratación, Financiera, Gestión Documental, Administrativa, talento Humano, y el Jefe de la Oficina de Sistemas de Información, quienes bajo este rol realizan seguimiento a la gestión del riesgo, orientan a la Primera Línea de Defensa sobre la implementación de los controles y buenas prácticas para la mitigación de las causas generadoras de los riesgos en los procesos, y alertan a la Alta Dirección sobre la eficacia de la gestión del riesgo.

La Oficina de Sistemas de Información como Segunda Línea de defensa monitorea los riesgos de seguridad y privacidad de la información.

La frecuencia del monitoreo se establece en la siguiente tabla:

Zona de Riesgo Residual	Periodicidad	
	Riesgos Gestión, Fiscales y de Seguridad de la Información	Riesgos de Corrupción
Bajo	SEMESTRAL	CUATRIMESTRAL
Moderado		
Alto	CUATRIMESTRAL	
Extremo		

Tabla 13. Frecuencia de monitoreo de Riesgo Residual.

NOTA:
Los monitoreos a los riesgos de gestión y fiscales se dejan registrados en el formato Matriz Riesgos de Gestión y Fiscales **DE-FM-022**.

Los monitoreos a los riesgos de corrupción se dejan registrados en el formato Matriz Riesgos de Corrupción **DE-FM-043**.

Los monitoreos a los riesgos de seguridad y privacidad de la información se dejan registrados en el formato **GTI-FM-024**.

Para los Riesgos de Corrupción, la Oficina Asesora de Planeación Sectorial publica en la página web institucional antes del 31 de enero de cada vigencia, la **DE-FM-043** Matriz de Riesgos, así como cada cuatrimestre los seguimientos realizados a estos.

Para los riesgos de gestión y fiscales, así como los de seguridad y privacidad de la información, la publicación de estos se dispone en la página web del ministerio. Así como en las caracterizaciones de los procesos.

- **Evaluación tercera línea de defensa:**

Por su parte la Oficina de Control Interno como tercera línea de defensa evalúa los riesgos a través de las auditorías, evaluaciones y seguimientos en desarrollo del plan anual de auditorías y seguimientos definidos para la vigencia.

Nota: En cuanto a la 2ª Línea de Defensa, lleva a cabo autoevaluación permanente de las actividades llevadas a cabo por la 1ª línea de defensa, por lo que su objetivo principal es asegurar que la primera línea está diseñada y opera de manera efectiva, es decir, que las funciones de la segunda línea de defensa informan a la Alta Dirección y/o son parte de la Alta Dirección y generan información clave para la toma de decisiones en tiempos diferenciados respecto de los seguimientos y evaluaciones de la tercera línea de defensa y con respecto a temas o aspectos transversales en la entidad[20]

1. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se evidencian riesgos materializados identificados durante las actividades de monitoreo y seguimiento (autoevaluación por parte del líder del proceso, o de los líderes de los sistemas de gestión implementados, auditorías internas y externas a los sistemas de gestión, auditorías de gestión y seguimientos de la Oficina de Control Interno, auditorias de los entes de control, peticiones, quejas, reclamos, sugerencias o denuncias, PQRSD, entre otras), se deben aplicar las acciones descritas en la siguiente tabla:

RESPONSABLE	ACCIÓN
Primera Línea de Defensa (Líder de Proceso)	• Informar a la Oficina Asesora de Planeación Sectorial y al líder del sistema de gestión implementado, sobre el hecho encontrado que evidencia la materialización del riesgo. • Para la materialización de los riesgos de **corrupción**, una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción), tramitar la denuncia ante la instancia de control correspondiente. • Para los riesgos de **seguridad y privacidad de la información** reportar oportunamente el evento o incidente para la adecuada gestión e implementar las medidas pertinentes que permitan contenerlo y garantizar la continuidad del servicio (si es el caso). • Identificar las **acciones correctivas** necesarias y documentarlas en el módulo de mejora, de ISOLUCION. • Efectuar el análisis de causas y determinar acciones correctivas. • Implementar y realizar seguimiento a las acciones correctivas formuladas • Revisar el riesgo materializado en sus diferentes etapas, actualizarlo en caso de ser necesario y divulgarlo a las partes interesadas
Segunda Línea de Defensa (OAPS, secretaria general y líderes de los Sistemas de Gestión)	• Asesorar a los líderes de los procesos para la documentación de las acciones correctivas. • Acompañar a los líderes de los procesos en la revisión del riesgo materializado y en la actualización del mapa de riesgos. • Llevar el listado de los riesgos materializados en el formato DE-FM-024 Listado de Riesgos Materializados. • Solicitar la publicación de las matrices de riesgos, en la página web y/o sitio definido para tal fin, en caso de que se hayan presentado cambios en alguna de las etapas del riesgo materializado.
Tercera Línea de Defensa (Oficina de Control Interno)	• Informar al Líder del Proceso del riesgo materializado. • Informar a la segunda línea de defensa del riesgo materializado, con el fin de facilitar el inicio de las acciones correctivas correspondientes con el líder del proceso y la revisión del riesgo materializado. • Recomendar al líder del proceso en la revisión, análisis y formulación de acciones correctivas. • Verificar que se tomaron las acciones correctivas pertinentes y la actualización del mapa riesgo. • Para el riesgo de corrupción, una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.

Tabla 14. Acciones ante los riesgos materializados.

TÍTULO V. DOCUMENTACIÓN DE LOS RIESGOS

El Ministerio cuenta con los siguientes formatos donde se identifican, valoran, evalúan y administran los riesgos

- Matriz Riesgos de Gestión y Fiscal DE-FM-022
- Matriz Riesgos de Corrupción DE-FM-043
- Matriz Riesgos de Seguridad y privacidad de la información GTI-FM-024

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA VIGENCIA	RAZÓN DE LA ACTUALIZACIÓN
00	28/07/2020	Versión inicial. • Los documentos de riesgos estaban asociados al Proceso de Sistema de Gestión, de acuerdo con el objetivo pertenecen al Proceso de Direccionamiento Estratégico, por tal razón se trasladan. • Se crean los formatos DE-FM-022 Matriz de Riesgos, DE-FM-023 Matriz de Oportunidades • Aprobado en Comité Institucional de Coordinación de Control Interno, mediante Acta 02, del 28 de julio de 2020 • Con la creación de este documento se **eliminan** los siguientes documentos, que hacían parte del proceso de Sistema de Gestión: SG-PR-017 Procedimiento Gestión del Riesgo_v2 ES-GU-001 Guía para la Administración del Riesgo_v2 SG-FM-043 Matriz de identificación y seguimiento a mapas de riesgov6 SG-FM-067 Formulación y Monitoreo Mapa de Riesgos de Corrupción_v10 SG-FM-042 Plan de Contingenciav4 Resolución 1900 del 03 de octubre de 2016
01	27/05/2021	Se hacen las siguientes actualizaciones al documento según los nuevos lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de diciembre de 2020: - Actualización de definiciones: - Se incluye medición para: Apetito al riesgo, tolerancia al riesgo, Capacidad de riego. - Se modifica la forma como se debe describir el riesgo. - Se adicionan algunas recomendaciones para la redacción del riesgo. - Se modifica el cuadro de clasificación del riesgo - Se modifica la valoración en la tabla de probabilidad - Se modifica la valoración en la tabla de impacto - Se modifican los mapas de Calor - Se incluye el control correctivo - Se modifican las etapas para la redacción de un control - Se incluye control manual y control automático - Se modificó la tabla de calificación de atributos para el diseño de los controles - Se incluye la fórmula para hallar el nivel de riesgo residual - Se modifica la tabla de niveles de aceptación de riesgo residual - Se modifica la tabla para monitoreo de riesgo residual - Se incluyen los formatos DE-FM-022 Matriz Riesgos, DE-FM-023 Matriz Oportunidades y DE-FM-024 Listado de Riesgos Materializados, Resolución 0894 del 30 de agosto de 2021: Por la cual se actualiza y adopta la Política y Metodología para la Administración de Riesgos y Oportunidades del Ministerio de Comercio, Industria y Turismo.

02	02/03/2023	Se realizan los siguientes cambios, luego de revisado el documento. - Se incluye definición de Activo, Análisis de riesgo, Ciberseguridad, Impacto, Identificación del Riesgo, Riesgos en seguridad de la información y Valoración del riesgo. - Se complementa la definición de Amenazas. - En el numeral 5. CONDICIONES GENERALES, se suprime los riesgos del proceso del sistema de gestión y se dejan por separado los riesgos de cada subsistema. - En el numeral 5. CONDICIONES GENERALES, se incluye el sistema de gestión ambiental. - En el título II, capítulo 2 CLASIFICACIÓN DEL RIESGO, en los riesgos de seguridad de la información, se incluye en la descripción "*Pérdida de confidencialidad – privacidad"* - En la tabla 2 Clasificación del riesgo, se clasifican los riesgos de fraude interno y fraude externo como clases de riesgo de gestión. - En el título II, capítulo 3 DESCRIPCIÓN DEL RIESGO, se elimina la palabra "POSIBILIDAD", al momento de redactar el riesgo. - En el título II, capítulo 3 DESCRIPCIÓN DEL RIESGO, literal 3.2 riesgos de seguridad de la información, se modifica la redacción. - Se elimina la palabra consecuencia que acompaña al impacto, al igual que fraude como acompañante de corrupción. - En el numeral 5. NIVELES DE ACEPTACIÓN DEL RIESGO RESIDUAL, se incluye en el Nivel del Riesgo Residual, "Se deben establecer acciones de mejora o correctivas según sea el caso", para los riesgos residuales con severidad extrema o alta. - En el título IV. MONITOREO Y SEGUIMIENTO A LOS RIESGOS, en el numeral 1. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS, se modifica la acción para la primera línea de defensa con respecto a los riesgos de seguridad de la información. - Se separa el riesgo de Fraude del riesgo de Corrupción.
03	14-03-2024	Se realizan los siguientes cambios: - DEFINICIONES: se incluyen Actualización de definiciones en el tema de riesgos fiscales, de acuerdo a la Guía del DAFP en su última versión. - En el punto 5. CONDICIONES GENERALES, se eliminó la información relacionada con el nombre Sistema de Gestión de Calidad. - MARCO CONCEPTUAL PARA NIVELES DE ACEPTACIÓN DEL RIESGO se incluye niveles de aceptación para riesgos fiscales. - CLASIFICACIÓN DEL RIESGO: se incluye la clasificación del riesgo fiscal - DESCRIPCIÓN DEL RIESGO: se complementó la información para ajustar la descripción de los riesgos de gestión y de corrupción, y se incluyó la descripción para riesgo fiscal. - VALORACIÓN, se ajusta la tabla en sus parámetros para la

		valoración del impacto, de acuerdo con los lineamientos de la guía del DAFP, en su versión vigente. - En el título III, numeral 3. DISEÑO Y VALORACIÓN DE CONTROLES, se complementa la información de los elementos para la determinación del control y su correcta redacción. Adicionalmente, se definen las tres (3) tipologías para el diseño del control. Se adiciona la tabla para la valoración de los controles de los riesgos de corrupción. - NIVELES DE ACEPTACIÓN DEL RIESGO RESIDUAL se incluye los niveles de aceptación para los riesgos fiscales, se ajustó la tabla, parametrizando la generación de planes de acción y definición de indicadores para medir su eficacia y su efectividad. Así mismo se elimina la necesidad de establecer indicadores para los niveles de riesgo mencionados anteriormente. - En el título IV. MONITOREO Y EVALUACIÓN A LOS RIESGOS, se ajustan las responsabilidades para la primera y segunda línea de defensa de acuerdo a lo dispuesto en la Guía del DAFP en su última Versión 6. Se crea la plantilla para el monitoreo a los riesgos de corrupción. - ACCIONES ANTE LOS RIESGOS MATERIALIZADOS se ajustan las responsabilidades de la primera y segunda línea de defensa - DOCUMENTACIÓN DE LOS RIESGOS se crea el formato para la matriz de riesgos de corrupción DE-FM-043 y matriz de riesgos de Seguridad y Privacidad de la Información GTI-FM-024 - BIBLIOGRAFÍA, se referencia la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, en sus versiones 4 y 6. - ADMINISTRACIÓN DE OPORTUNIDADES. Se elimina este capítulo, dado que este se encontraba bajo el Sistema Integrado de Gestión, y el ministerio ya no opera bajo este sistema, por cuanto acoge el Modelo Integrado de Operación -MIO-, el cual no contempla lineamiento alguno al respecto. Adicionalmente, la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, no lo refiere. - Se ajusta el nombre del documento teniendo en cuenta el punto anterior, quedando *"Política y Metodología para la administración de Riesgos"*
04	26/11/2024	Se realizan los siguientes cambios: **TITULO III. VALORACIÓN DEL RIESGO** - 1.1 Determinar la PROBABILIDAD: se ajustan los criterios para valorar la probabilidad de ocurrencia de los riesgos de corrupción (columna frecuencia de eventos) - Determinar el IMPACTO: se ajustan los criterios para valorar el impacto económico y reputacional en los riesgos fiscales y de gestión.

REVISIÓN Y APROBACIÓN DEL DOCUMENTO

	ELABORÓ	REVISÓ	APROBÓ
Nombre:	Rodrigo Jiménez Mónica Vargas	Diana Larisa Caruso	Aprobado en Comité Institucional de Coordinación de Control Interno, mediante Acta 02 de noviembre 2024.
Cargo:	Asesor de Planeación Sectorial Contratista Riesgos	Jefe Oficina Asesora de Planeación Sectorial	
Fecha de vigencia del documento:		26 de noviembre de 2024	

BIBLIOGRAFÍA

- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 4, octubre de 2018 (Descripción riesgos de corrupción).

- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 6, de noviembre de 2022 y anexos

ANEXO 1. RESPONSABILIDADES POR LÍNEA DE DEFENSA PARA LA ADMINISTRACIÓN DEL RIESGO[16]

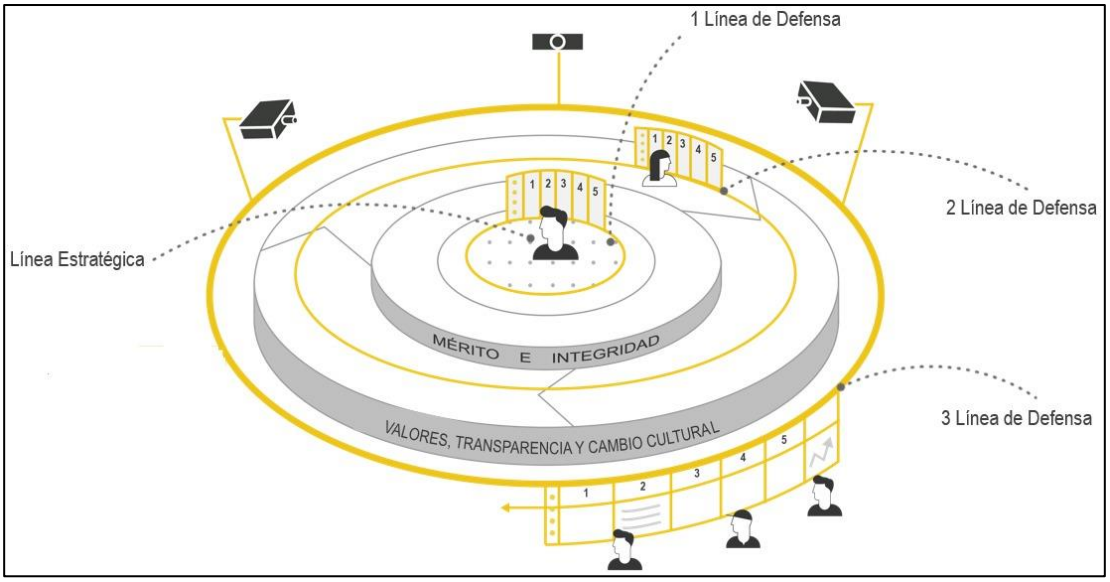


Figura 10. Esquema de líneas de defensa

En el Ministerio las responsabilidades de carácter general por líneas de defensa para la administración de riesgos, se detallan a continuación:

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
LINEA ESTRATÉGICA	Define el marco general para la gestión del riesgo y su control analiza los riesgos, monitorea la gestión y garantiza el cumplimiento de los planes estratégicos de la entidad (Objetivos, metas, indicadores)	**Al Ministro(a), equipo directivo (Secretario General, Viceministros, Directores) y al Comité Institucional de Coordinación de Control Interno les corresponde:**	**Por parte del Comité de Coordinación de Control Interno:** • Someter a aprobación del representante legal la política de administración del riesgo. • Revisar la exposición de la entidad a los riesgos de corrupción y gestión (fraude); si se cuenta con la línea de denuncia, monitorear el progreso de su tratamiento. • Verificar el cumplimiento de los lineamientos establecidos en la política de administración del riesgo, con énfasis en los de gestión (fraude) y corrupción.
			Monitorear permanentemente los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI.

[16] Las responsabilidades para la administración del riesgo se definieron con base en las líneas de defensa descritas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, anexo 7 criterios diferenciales.

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
			Monitorear el estado de los riesgos aceptados (apetito por el riesgo) con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad.
			Monitorear al cumplimiento de la política de administración del riesgo de la entidad.
			Analizar el resultado de las evaluaciones de la gestión del riesgo, elaboradas por la segunda y tercera líneas de defensa, para determinar el estado del SCI y definir los ajustes o modificaciones a que haya lugar.
PRIMERA LINEA DE DEFENSA	Desarrolla e implementa los procesos de control y gestión de riesgos, y detecta deficiencias (a través de su identificación, análisis, valoración, monitoreo, el control de una base del día a día de acciones de mejora.)	**Líderes de los procesos y sus equipos de trabajo (en general servidores públicos en todos los niveles del Ministerio), les corresponde:**	Identificar los activos de información de su proceso.
			Identificar, valorar y definir la opción de tratamiento de los riesgos (gestión, fiscales, corrupción, seguridad digital, fraude, financieros, entre otros) que pueden afectar el logro de los objetivos de los procesos, programas o proyectos en los cuales participe, acorde con la política de administración del riesgo.
			Identificar cambios que incidan en los riesgos y proponer los ajustes correspondientes.
			Identificar la posibilidad de fraude en los procesos, programas o proyectos en los cuales participe e informar oportunamente.
			Revisar en coordinación con la segunda línea de defensa en la identificación de riesgos.
			Definir y diseñar los controles que aplican (manuales o apoyados en TI) para gestionar los riesgos, identificando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución. (Ver Guía de Administración del Riesgo de Gestión, Corrupción y Seguridad Digital y Diseño de Controles para Entidades Públicas).
			Elaborar los mapas de riesgo, que incluyan los riesgos de gestión, fiscales, corrupción, fraude y de seguridad digital, entre otros.
			Identificar cambios en los riesgos establecidos y proponer ajustes a los controles.
			Efectuar seguimiento a los riesgos y la efectividad de los controles de los procesos, determinar y proponer posibles mejoras en los mismos, de acuerdo a las frecuencias establecidas
			Cumplir con las políticas y lineamientos para generar y comunicar la información relevante, de manera accesible, oportuna, confiable, íntegra y segura, que facilite las acciones de control en la entidad.

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
SEGUNDA LINEA DE DEFENSA	*Soporta y guía la línea estratégica *Supervisa, asegura y monitorea de manera independiente la pertinencia y eficacia en el cumplimiento de la gestión de riesgos de la primera línea que pueda afectar el cumplimiento de los objetivos estratégicos o de los procesos. *Ayuda a los responsables de riesgos a distribuir la información adecuada sobre el riesgo a todos los servidores de la entidad.	**El Jefe de la Oficina Asesora de Planeación Sectorial y líderes de los Sistemas de Gestión implementados en el Ministerio** **Jefe de Oficina Sistemas de Información**	Evaluar y proponer modificaciones frente al diseño y desarrollo de la política para la Gestión de Riesgos, con el fin de mantenerla actualizada.
			Generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno acerca del cumplimiento de las metas y los objetivos en relación a la gestión integral del riesgo.
			Evaluar y proponer estrategias de Gestión de Riesgos al Comité Institucional de Coordinación de Control Interno.
			Revisar las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos, áreas geográficas y tipos de riesgo (monitoreo del contexto estratégico).
			Supervisar y controlar el cumplimiento y la aplicación de políticas, límites y metodologías para gestionar los riesgos.
			Verificar en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas.
			Verificar la adecuada identificación de los riesgos relacionados con gestión (fraude) y corrupción.
			Generar recomendaciones a las instancias correspondientes (primera, segunda, y línea estratégica), a partir de la información relacionada con la verificación a la identificación y valoración del riesgo.
			Analizar y verificar la adecuada identificación de los riesgos en relación con los objetivos institucionales o estratégicos y de los procesos, definidos desde el Direccionamiento Estratégico.
			Revisar en coordinación con la primera línea de defensa en la identificación de riesgos.
			Asegurar que los riesgos son monitoreados acorde con la política de administración de riesgo establecida para la entidad.
			Verificar el diseño y ejecución de los controles que mitigan los riesgos estratégicos o institucionales.
			Verificar el diseño y ejecución de los controles que mitigan los riesgos de gestión (fraude) y corrupción.
			Hacer seguimiento a los mapas de riesgo y verificar su actualización de acuerdo a los cambios establecidos en la Política de Riesgos Institucional.
			El Oficial de Seguridad de la Información verifica el desarrollo y mantenimiento de controles de

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
			Tecnológicos y de seguridad y privacidad de la información
			Revisar en coordinación con la tercera línea de defensa la efectividad de los controles.
			Verificar que el diseño del control establecido por la primera línea de defensa sea pertinente frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y efectuar las recomendaciones a que haya lugar ante las instancias correspondientes (primera, segunda, y línea estratégica).
			Verificar que los responsables estén ejecutando los controles tal como han sido diseñados.
			Verificar que los controles contribuyen a la mitigación de riesgos hasta niveles aceptables.
			Evaluar la gestión del riesgo de la entidad con énfasis en: *La exposición al riesgo, acorde con los lineamientos y la política institucional, *El cumplimiento legal y regulatorio, *Logro de los objetivos estratégicos o institucionales, *Confiabilidad de la información financiera y no financiera.
			Como resultado de la evaluación de la gestión del Riesgo comunica las deficiencias a la alta dirección o a las partes responsables para tomar las medidas correctivas, según corresponda.
			Revisar con la primera línea la adecuada formulación de los planes de mejoramiento y generar recomendaciones (análisis de causas, acciones, responsables y tiempos).
			Verificar el avance y cumplimiento de las acciones incluidas en los planes de mejoramiento producto de las autoevaluaciones.
TERCERA LINEA DE	Provee aseguramiento independiente y objetivo sobre la efectividad en el cumplimiento de las responsabilidades de la línea estratégica, la primera y segunda línea de defensa con relación a la	**Al Jefe de Control Interno, le corresponde:**	Verificar y evaluar que la entidad haya definido una política de administración del riesgo, atendiendo los lineamientos establecidos en la metodología adoptada por la entidad (Rol Enfoque hacia la prevención).
			Evaluar y alertar oportunamente sobre cambios que afecten la exposición de la entidad a los riesgos de corrupción y gestión (fraude). (Rol Enfoque hacia la prevención).
			Evaluar el cumplimiento de la política de administración del riesgo en todos los niveles de la entidad. (Rol Evaluación de la Gestión del Riesgo).
			Identificar y alertar al Comité de Coordinación de Control Interno posibles cambios que pueden afectar

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
	gestión de riesgos; a través de (evaluación) auditorías internas de control a la alta dirección de la entidad, en donde se valida que la gestión de riesgos es adecuada al logro de los objetivos institucionales y de los procesos		la evaluación y tratamiento del riesgo. (Rol Evaluación de la Gestión del Riesgo).
			Evaluar las actividades adelantadas por la segunda línea de defensa frente a la gestión del riesgo (oficina de planeación, direcciones o gerencias de riesgo), específicamente frente al análisis de contexto y de identificación del riesgo y de ser necesario asesorarlas, a fin de incorporar las mejoras correspondientes. (Rol Evaluación de la Gestión del Riesgo).
			Evaluar la efectividad de los controles, a partir de resultado del análisis del diseño, ejecución y la no materialización de los riesgos, y generar los informes ante las instancias correspondientes (primera, segunda, y línea estratégica). Se incluyen los controles tecnológicos y relacionados con riesgos de seguridad digital, los de gestión (fraude) y de corrupción. (Rol de Evaluación de la Gestión del Riesgo).
			Evaluar que el diseño del control establecido sea adecuado frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y generar los informes ante las instancias correspondientes (primera, segunda, y línea estratégica). Se incluyen los controles tecnológicos y relacionados con riesgos de seguridad digital, los de gestión (fraude) y de corrupción. (Rol de Evaluación de la Gestión del Riesgo).
			Evaluar que los mapas de riesgos se encuentren actualizados. (Rol de Evaluación de la Gestión del Riesgo).
			Evaluar en coordinación con la segunda línea de defensa la efectividad de los controles. (Rol de Evaluación y Seguimiento).
			Establecer y ejecutar el plan anual de auditoría basado en riesgos, priorizando aquellos procesos de mayor exposición, así como la verificación del funcionamiento de los componentes de control interno e informar las deficiencias de forma oportuna a las partes responsables de aplicar las medidas correctivas (Línea estratégica, primera y segunda línea de defensa). (Rol de Evaluación y Seguimiento)
			Evaluar la efectividad de las acciones desarrolladas por la segunda línea de defensa en aspectos como: cobertura de riesgos, cumplimientos de la

LÍNEA	PROPÓSITO	RESPONSABLE	ACTIVIDADES
			planificación, mecanismos y herramientas aplicadas, entre otros, y generar observaciones y recomendaciones para la mejora. (Rol de Evaluación y Seguimiento).