

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	1 de 52

## 1. OBJETIVO

Generar una visión sistémica acerca de la administración y evaluación de riesgos dentro de los procesos y procedimientos de la Institución, propendiendo por la protección de los recursos de la organización a través de la generación de acciones y mecanismo que disminuyan la probabilidad o el impacto en la materialización de los riesgos.

## 2. ALCANCE

Este procedimiento aplica a todos los procesos de la Institución.

## 3. RESPONSABLE

Director de Planeación y mejoramiento de la calidad

## 4. DEFINICIONES

**Administración de Riesgos:** Conjunto de Elementos de Control que, al interrelacionarse, permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.

**Riesgo De Gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

**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.

**Oportunidad:** Posibilidad de lograr algún tipo de mejora en los procesos

**Riesgo Inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

**Riesgo Residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento

**Análisis de Riesgo:** Elemento de Control, que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo.

**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.

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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	2 de 52

**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

**Contexto Estratégico:** factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de sus objetivos.

**Control:** Es toda acción que tiende a minimizar los riesgos

**Identificación de Riesgos:** 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.

**Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

**Indicador:** Es la valoración de una o más variables que informa sobre una situación y soporta la toma de decisiones, es un criterio de medición y de evaluación cuantitativa o cualitativa

**Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

**Riesgo:** Probabilidad de ocurrencia de un evento o fenómeno positivo o negativo que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos. (Entiéndase positivo como una oportunidad o negativo como una amenaza).

**Valoración del Riesgo:** Elemento de Control, que determina el nivel o grado de exposición de la entidad pública al impacto del riesgo, permitiendo estimar las prioridades para su tratamiento.

**Tolerancia Al Riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

## 5. CONTENIDO

### 5.1 GENERALIDADES

El nivel directivo y los responsables de procesos identifican los factores internos y externos que afectan el normal desarrollo de los procesos y actividades de la Institución, como los económicos, políticos, sociales, tecnológicos, financieros, laborales, legales, logísticos, etc., que pueden generar eventos, que originen oportunidades o afecten negativamente el cumplimiento de la misión, funciones y objetivos Institucionales.

Este elemento se realiza tomando como base el Diagnostico Estratégico Institucional diseñado a partir del análisis DOFA.

Los objetivos de los procesos son el punto de partida fundamental para la identificación de riesgos y oportunidades.

Matriz DOFA Umayor: <https://umayor.edu.co/planeacion/planeacion-y-calidad-academica/>

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	3 de 52

## 5.2 PASO A PASO

### 1. DEFINIR POLÍTICA DE ADMINISTRACION DE RIESGOS

#### ¿QUÉ ES?

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

#### ¿QUIÉN LA ESTABLECE?

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

### POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

#### ¿QUÉ SE DEBE TENER EN CUENTA?

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

#### ¿QUÉ DEBE CONTENER?

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

*Ilustración 1 Estructuración de la política de administración de riesgos*

*Fuente: Guía administración del riesgo Función pública*

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	4 de 52

## 2. IDENTIFICACION DEL RIESGO

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

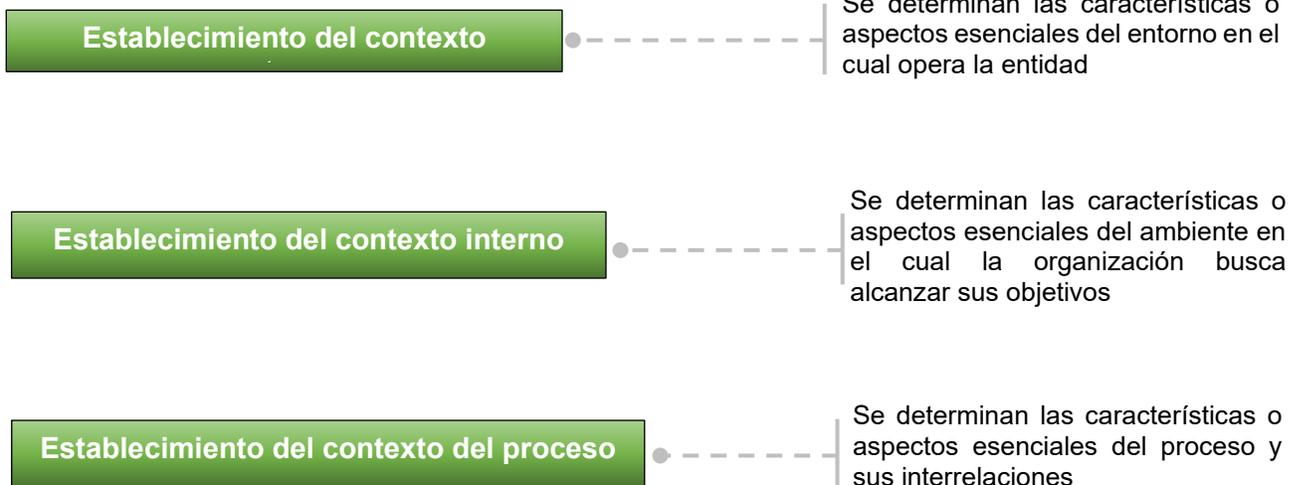
La segunda línea de defensa (Compuesta por planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, comité de contratación, áreas financieras, de TIC, entre otros que generen información para el Aseguramiento de la operación.) le corresponden el análisis de los objetivos de la entidad tanto estratégicos como de procesos.

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

### 2.1 Establecimiento del contexto

La institución definirá los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

*Análisis del contexto interno, externo y del proceso*



<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	5 de 52

Para definir el contexto interno, externo y de proceso se pueden considerar los siguientes factores:

Factores para cada categoría de riesgos:

- **Contexto interno y de proceso**

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	6 de 52

### Factor externo

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

*Ilustración 2 Análisis del contexto  
Fuente: Función Pública, 2020.*

## 2.2 Identificación de riesgos

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. 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 los estratégicos. Las preguntas claves para la identificación del riesgo permiten determinar:

**¿QUÉ PUEDE SUCEDER?** Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

**¿CÓMO PUEDE SUCEDER?** Establecer las causas a partir de los factores determinados en el contexto.

**¿CUÁNDO PUEDE SUCEDER?** Determinar de acuerdo con el desarrollo del proceso.

**¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?** Determinar los posibles efectos por la materialización del riesgo.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	7 de 52

### 2.2.1 Técnicas de redacción de riesgos

Evitar iniciar con palabras negativas como: “No”, “Que no”, o con palabras que denoten un factor de riesgo (causas) como “Ausencia de”, “Falta de”, “Poco (a)”, “Escaso (a)”, “Insuficiente”, “Deficiente”, “Debilidades en”



Objetivo del proceso: Todos los riesgos identificados deben estar asociados al objetivo del proceso Pregúntese si el riesgo de gestión identificado está relacionado directamente con las características del objetivo. Si la respuesta es NO, este puede ser la causa o consecuencia

Generar al lector o escucha la imagen del evento como si ya estuviera sucediendo



- **Ejemplo:**

PROCESO	OBJETIVO	RIESGO	DESCRIPCION	CAUSA	CONSECUENCIA
Contratación y compras	adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	La combinación de factores como insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad y, en consecuencia, afectar la continuidad de su operación.	1.Carencia de controles en el procedimiento de contratación 2.Insuficiente capacitación del personal de contratos 3.Desconocimiento de los cambios en la regulación contractual 4.Inadecuadas políticas de operación	1.Parálisis en los procesos 2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor 3. Demandas y demás acciones jurídicas 4. Detrimiento de la imagen de la entidad ante sus grupos de valor 5. Investigaciones disciplinarias

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	8 de 52

### 3. VALORACIÓN DEL RIESGO

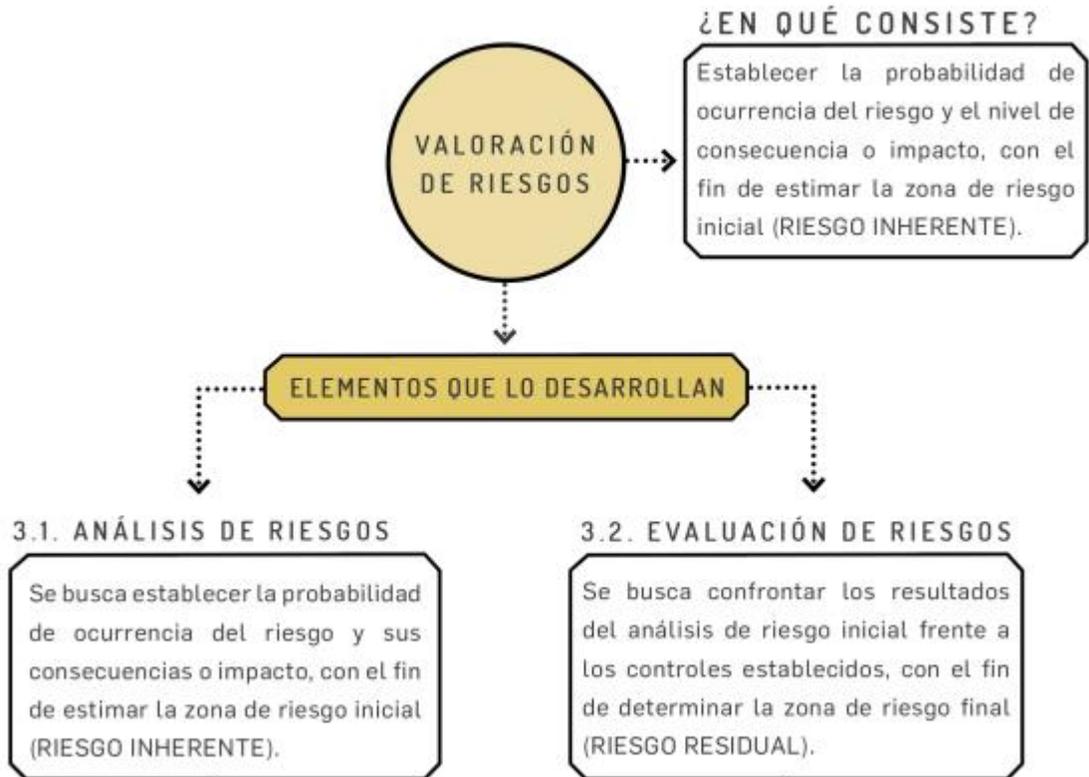


Ilustración 3 estructura para el desarrollo de la valoración del riesgo  
Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

#### 3.1 Análisis del riesgo

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

- Determinar la probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.  
 Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	9 de 52

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

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

- **Análisis de causas**

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos



Diagrama de Pareto



Espina de Pescado



Análisis de árbol de fallos



Arboles de decisión



5 porqué



Delphi



Matriz de Priorización

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	10 de 52

- **Determinar el impacto**

Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo. Se tienen en cuenta las consecuencias potenciales establecidas y la siguiente tabla.

TABLA DE IMPACTO			
Nivel	Descriptor	DESCRIPCIÓN	
		Impacto (Consecuencias) Cuantitativos	Impacto (Consecuencias) Cualitativas
1	Insignificante	<p>Impacto que afecte la ejecución presupuestal en un valor <math>\geq 0,5\%</math>.</p> <ul style="list-style-type: none"> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 1\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 0,5\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 0,5\%</math> del presupuesto general de la entidad.</li> </ul>	<p>No hay interrupción de las operaciones de la entidad.</p> <ul style="list-style-type: none"> <li>- No se generan sanciones económicas o administrativas.</li> <li>- No se afecta la imagen institucional de forma significativa.</li> </ul>
2	Menor	<p>Impacto que afecte la ejecución presupuestal en un valor <math>\geq 1\%</math>.</p> <ul style="list-style-type: none"> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 5\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 1\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 1\%</math> del presupuesto general de la entidad.</li> </ul>	<p>Interrupción de las operaciones de la entidad por algunas horas.</p> <ul style="list-style-type: none"> <li>- Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias.</li> <li>- Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos</li> </ul>
3	Moderado	<p>Impacto que afecte la ejecución presupuestal en un valor <math>\geq 5\%</math>.</p> <ul style="list-style-type: none"> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 10\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 5\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 5\%</math> del presupuesto general de la entidad.</li> </ul>	<p>Interrupción de las operaciones de la entidad por un (1) día.</p> <ul style="list-style-type: none"> <li>- Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.</li> <li>- Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios.</li> <li>- Reproceso de actividades y aumento de carga operativa.</li> <li>- Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.</li> <li>- Investigaciones penales, fiscales o disciplinarias.</li> </ul>

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	11 de 52

4	Mayor	<p>Impacto que afecte la ejecución presupuestal en un valor <math>\geq 20\%</math>.</p> <ul style="list-style-type: none"> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 20\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 20\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 20\%</math> del presupuesto general de la entidad.</li> </ul>	<p>Interrupción de las operaciones de la entidad por más de dos (2) días.</p> <ul style="list-style-type: none"> <li>- Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.</li> <li>- Sanción por parte del ente de control u otro ente regulador.</li> <li>- Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.</li> <li>- Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.</li> </ul>
5	Catastrófico	<p>Impacto que afecte la ejecución presupuestal en un valor <math>\geq 50\%</math>.</p> <ul style="list-style-type: none"> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 50\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 50\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 50\%</math> del presupuesto general de la entidad</li> </ul>	<p>Interrupción de las operaciones de la entidad por más de cinco (5) días.</p> <ul style="list-style-type: none"> <li>- Intervención por parte de un ente de control u otro ente regulador.</li> <li>- Pérdida de información crítica para la entidad que no se puede recuperar.</li> <li>- Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.</li> <li>- Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.</li> </ul>

- **Análisis del impacto**

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

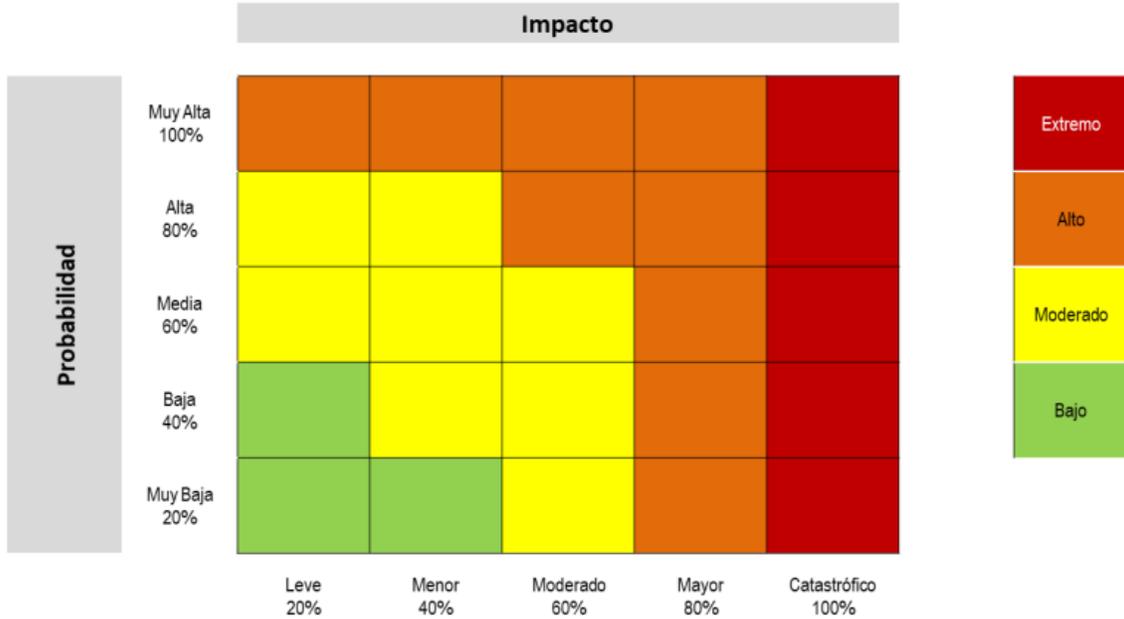
- **Mapa de calor**

Se toma la calificación de probabilidad resultante de la tabla “Matriz de priorización de probabilidad”, para este ejemplo se tomará la probabilidad de ocurrencia en “probable” y la calificación de Impacto en “mayor”, ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (R1), así se podrá determinar el riesgo inherente.

Matriz de criticidad de 5x5 significa que para ubicar el nivel de riesgo se cuenta con 5 niveles en probabilidad y 5 niveles en impacto.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	12 de 52



Zona de riesgo	Opciones de manejo del riesgo	
Baja	* Asumir el riesgo	Se asume el riesgo. Nota: Si el riesgo inherente se ubica en la zona baja, se debe revisar si este riesgo amerita o no, que se incluya en el mapa de riesgos, para su administración.
Moderada	* Asumir el riesgo * Reducir el riesgo	Se asume el riesgo. Se implementan controles y sus acciones de manejo del riesgo orientadas a disminuir la probabilidad de materialización del riesgo Y/O controles y sus acciones de manejo del riesgo, orientadas a disminuir el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a la zona baja.
Alta	* Reducir el riesgo * Evitar el riesgo * Compartir o transferir el riesgo	Se implementan controles y sus acciones de manejo del riesgo, orientadas a disminuir o evitar la materialización del riesgo Y/O controles y sus acciones de manejo del riesgo orientadas a disminuir o evitar el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a zona moderada. En lo relacionado con compartir o transferir el riesgo, se podría establecer el mantenimiento de pólizas (contratos de seguros), tercerización, entre otras; como controles o

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	13 de 52

		acciones de manejo del riesgo enfocadas a la protección. Esta opción de manejo se deberá tener en cuenta, con base en la capacidad del proceso y/o la entidad, para asumir las consecuencias del impacto producido por la materialización del riesgo.
<b>Extrema</b>	* Reducir el riesgo * Evitar el riesgo * Compartir o transferir el riesgo	Se implementan controles y sus acciones de manejo del riesgo, orientadas a disminuir o evitar la materialización del riesgo Y/O controles y sus acciones de manejo del riesgo orientadas a disminuir o evitar el impacto de la materialización del riesgo. En lo relacionado con Compartir o transferir el riesgo, teniendo en cuenta que en esta zona de riesgo se pueden producir pérdidas considerables para el proceso y/o la entidad, se hace necesario que se implementen controles de protección y sus acciones de manejo del riesgo, en los cuales se involucren pólizas, tercerizaciones, entre otras medidas que protejan el proceso y/o la entidad.

### 3.2 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 (RIESGO INHERENTE).

### 3.3 Valoración de los controles

en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

#### 3.3.1 Estructura para la descripción del control:

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

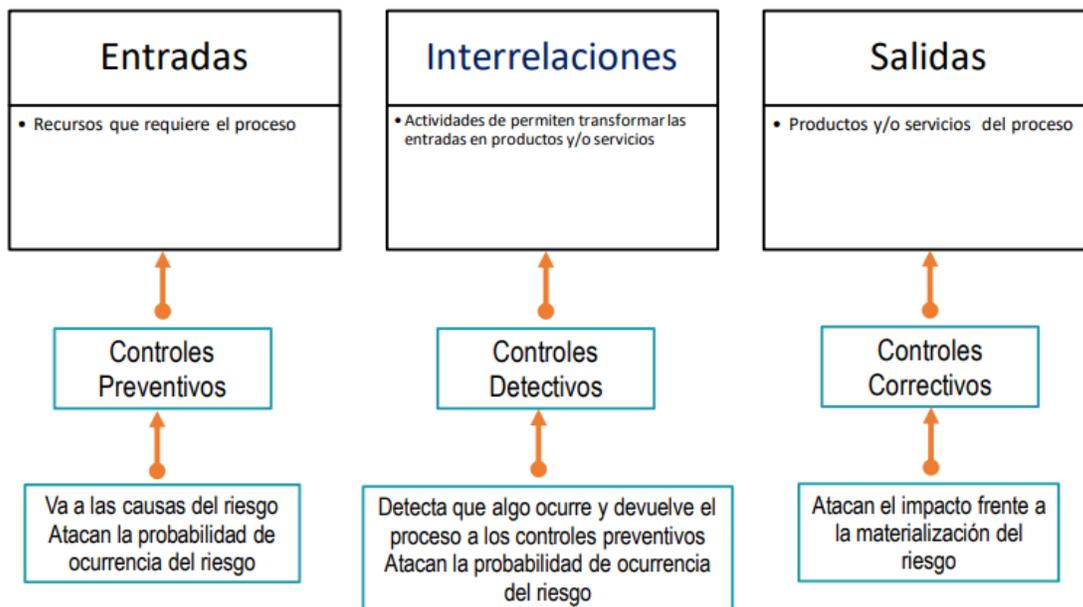
<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	14 de 52

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

### 3.3.2 tipología de los controles y los procesos

a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura 15 se consideran 3 fases globales del ciclo de un proceso así:



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

- Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	15 de 52

### 3.3.3 Valoración y diseño de controles

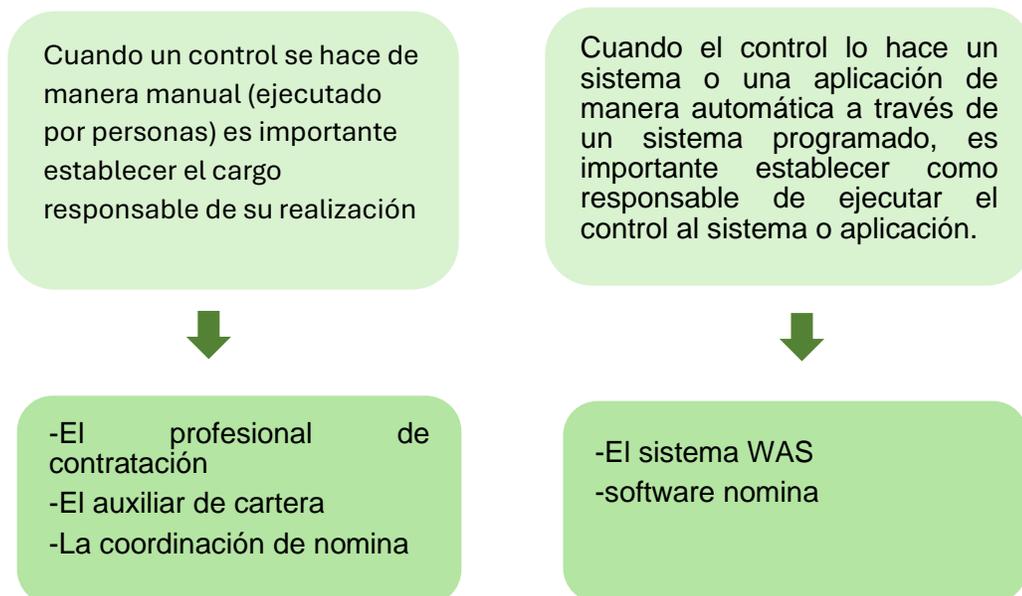
¿Cómo defino o establezco un control para que en su diseño mitigue de manera adecuada el riesgo?

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

#### Debe tener definido el responsable de llevar a cabo la actividad de control

- RESPONSABLE:** Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución.

Ejemplo:



- El control debe iniciar con un cargo responsable o un sistema o aplicación.
- Evitar asignar áreas de manera general o nombres de personas.
- El control debe estar asignado a un cargo específico.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	16 de 52

**Debe tener una periodicidad definida para su ejecución.**

- PERIODICIDAD:** El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o se detecta de manera oportuna el riesgo. Una vez definido el paso 1 - responsable del control, debe establecerse la periodicidad de su ejecución. Cada vez que se releva un control debemos preguntarnos si la periodicidad en que este se ejecuta ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada.

Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores solo se ejecutan cuando se contratan proveedores. La periodicidad debe quedar redactada de tal forma que indique: que cada vez que se desarrolla la actividad se ejecuta el control.

Ejemplo:

-El profesional de contratación:  
Cada vez que se va a realizar un contrato con el proveedor de servicios.

-El auxiliar de cartera:  
Mensualmente

-La coordinación de nómina:  
Mensualmente

De igual forma hay controles automáticos que son programados para que se ejecuten en un tiempo específico, estos controles también tienen una periodicidad

Todos los controles deben tener una periodicidad específica. Si queda a criterio la periodicidad de la realización del control, tendríamos un problema en el diseño del control.

- Debe indicar cuál es el propósito del control.**

El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas. Siguiendo las variables a considerar en la evaluación del diseño de control revisadas, veamos algunos ejemplos de cómo se deben redactar los controles, incluyendo el propósito del control, es decir, lo que este busca.

Al momento de identificar los controles para mitigar el riesgo, debemos preguntarnos si es una actividad o un control, y para diferenciarlo es importante tener en cuenta que el control (verifica, valida, concilia, coteja, compara, etc.) ayuda a la mitigación del riesgo,

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	17 de 52

por eso es importante que pensemos primero en tener controles preventivos antes que detectivos

Ejemplo:

\*Cada vez que se va a efectuar un contrato el profesional de contratación **verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación.**

\* El auxiliar de cartera mensualmente **verifica que los valores recaudados en 'Banco' correspondan con los saldos adeudados por los clientes.**

\*El director del programa cada Corte **Verifica los estudiantes reportados con dificultades académicas por parte de los docentes**

\*Cada vez que va a realizar un pago en el sistema SAP **valida que el proveedor al cual se le va a girar el pago no este reportado en lista restrictiva o de lavado de activos y financiación de territorio y financiación del terrorismo.**

\*Cada vez que se realizan las copias de seguridad el director de sistemas **valida que se haya guardado la información de todos los equipos de la institución**

El control debe tener un propósito (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo.

- **Debe establecer el cómo se realiza la actividad de control**

El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo. Cuando estemos evaluando el control debemos preguntarnos si la fuente de información utilizada es confiable. Ej.: para verificar los requisitos que debe cumplir un proveedor en el momento de ser contratado es mejor utilizar una lista de chequeo que hacerlo de memoria, dado que se nos puede quedar algún requisito por fuera.

Ejemplo:

\*Cada vez que se va a realizar un contrato el profesional de contratación verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación **a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor.**

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	18 de 52

- **Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control**

El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones

Ejemplo:

\*Cada vez que se va a realizar un contrato el profesional de contratación, verifica a través de una lista de chequeo que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación. **En caso de encontrar información faltante, requiere al proveedor a través de correo el suministro de la información y poder continuar con el proceso de contratación.**

Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones o desviaciones, el control tendría problemas en su diseño.

- **Debe dejar evidencia de la ejecución del control.**

El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente:

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo a la periodicidad definida.
3. Se cumplió con el propósito del control.
4. Se dejó la fuente de información que sirvió de base para su ejecución.
5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control

Ejemplo

\*Cada vez que se va a realizar un contrato, el profesional de contratación verifica a través de una lista de chequeo que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación. En caso de encontrar información faltante, solicita al proveedor por correo la información y poder continuar con el proceso de contratación.

**Evidencia: la lista de chequeo diligenciada, la información de la carpeta del cliente y los correos a que hubo lugar en donde solicitó la información faltante (en los casos que aplique).**

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	19 de 52

Hay controles en los que su evidencia queda en un flujo a través de una aplicación como un “aprobado” o “revisado” y otros en los que la evidencia es la configuración y programación de la aplicación, cuando es un control automático

Las acciones de tratamiento se agrupan en:

- \* Disminuir la probabilidad: acciones encaminadas a gestionar las causas del riesgo
- \* Disminuir el impacto: acciones encaminadas a disminuir las consecuencias del riesgo

Teniendo claro cómo se deben diseñar los controles procedimos a valorarlos:

- **Valoración de Controles**

Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas:

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

CRITERIO DE EVALUACION	ASPECTO PARA EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1.Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No Asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Asignado	No Asignado
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	Inoportuna
3.Proposito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	No es un control
4.Como 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.Que pasa con las	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del	Se investigan y resuelven	No Se investigan y resuelven

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	20 de 52

observaciones o desviaciones	control son investigadas y resueltas de manera oportuna?	oportuna	oportuna
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	Incompleta/N o existe

- **Peso o participación de cada variable en el diseño del control para la mitigación del riesgo**

CRITERIO DE EVALUACION	OPCIONES DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACION DEL DISEÑO DEL CONTROL
Asignación del responsable	Asignado	15
	No Asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15
	Detectar	10
	No es un control	0
Cómo se realiza la actividad de control	Confiable	15
	No Confiables	0
Qué pasa con las observaciones o desviaciones	Se investigan y se resuelven oportunamente	15
	No Se investigan y se resuelven oportunamente	0
Evidencia de la ejecución del control	Completa	15
	Incompleta	10
	No existe	0

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	21 de 52

De acuerdo con la puntuación obtenida según la tabla anterior el control se puede clasificar de la siguiente manera:

Rango de calificación del diseño	Resultado-peso en la evaluación del diseño del control	Peso de ejecución del control
Fuerte	Calificación entre 96 y 100	El control se ejecuta de manera consistente por parte del responsable
Moderado	Calificación entre 86 y 95	El control se ejecuta algunas veces por parte del responsable
Débil	Calificación entre 0 y 85	El control no se ejecuta por parte del responsable.

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría o control internos.

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

Dado que la calificación de riesgos inherentes y residuales se efectúa al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles.

En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

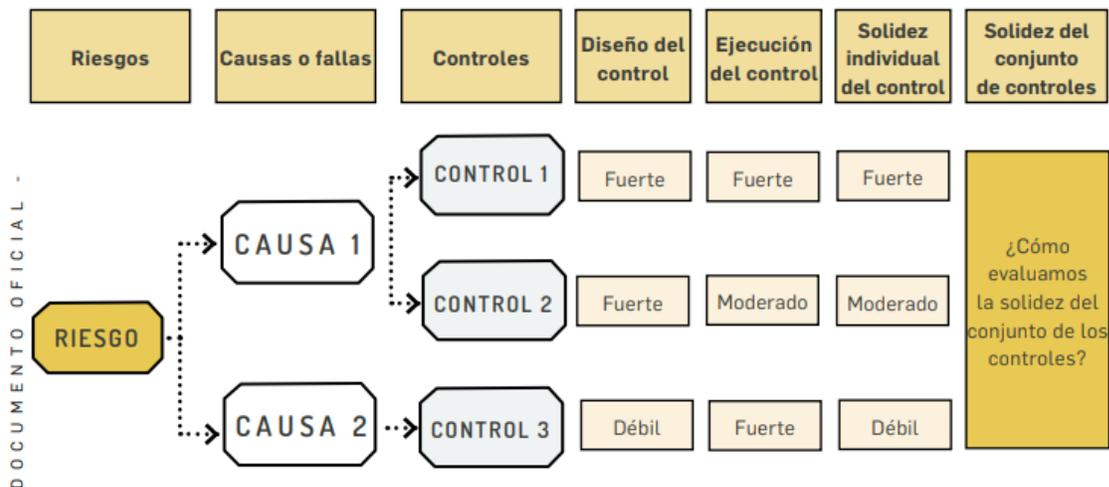
<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

Peso del diseño de cada control	Peso de la ejecución de cada control	Solidez individual de cada control Fuerte: 100, Moderado:50, Débil:0	Debe establecer acciones para fortalecer el control SI/NO
fuerte: calificación entre 96 y 100"	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

### Solidez del conjunto de controles para la adecuada mitigación del riesgo

Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.

### Solidez del conjunto de controles



<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	23 de 52

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.

- **Disminución de probabilidad e impacto.**

La mayoría de los controles que se diseñan son para disminuir la probabilidad de que ocurra una causa o evento que pueda llevar a la materialización del riesgo y muy pocos son dirigidos al impacto:

Ejemplo:

Para poder asignar un contrato se debe verificar que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación.

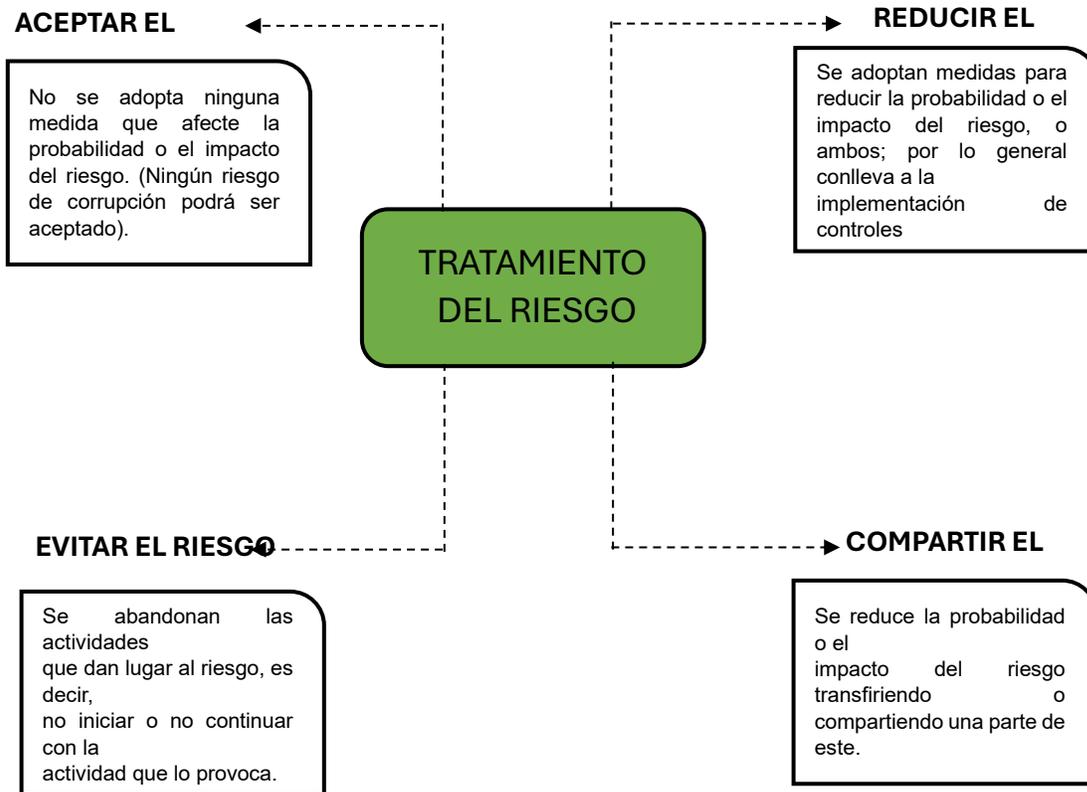
Generalmente se encuentran más controles que disminuyen directamente la probabilidad que el impacto. Si no existieran controles para disminuir la probabilidad del riesgo, el impacto de un riesgo por el número de eventos que se llegarían a materializar sería mayor, en nuestro ejemplo, si no existiera el control “verificar que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación para poder asignar un contrato”, el número de contratos que se incumplirían sería mayor, por tal razón, y para efectos de la elaboración de la matriz al momento de evaluar si los controles ayudan a disminuir el impacto o la probabilidad, estos controles se calificarán teniendo en cuenta que de manera indirecta disminuyen también el impacto.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	24 de 52

### Tratamiento del riesgo

El tratamiento del riesgo comprende un control. Estos valores del riesgo se conducen a niveles aceptables por la organización



<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	25 de 52

#### 4. Monitoreo y revisión

El modelo integrado de planeación y gestión (MIPG) desarrolla en la dimensión 7 el Modelo Estándar de Control Interno (MECI) y las líneas de defensa como eje articulador para identificar la responsabilidad de la gestión del riesgo y control. que está distribuida en diversos servidores de la entidad. La estructura del MECI busca una alineación a las buenas prácticas de control referenciadas desde el Modelo COSO, razón por la cual la estructura del MECI se fundamenta en cinco componentes, a saber: (i) ambiente de control, (ii) Evaluación del riesgo, actividades de control, (iv) información y comunicación y (v) actividades de monitoreo. Al respecto, el Manual Operativo MIPG v4, frente a dichos componentes establece lo siguiente:

“(…) El propósito para cada uno de los compontes se despliega de la siguiente forma:

1. **Ambiente de Control:** este componente busca asegurar un ambiente de control que le permita a la entidad disponer de las condiciones mínimas para el ejercicio del control interno. Requiere del compromiso, el liderazgo y los lineamientos de la alta dirección y del Comité Institucional de Coordinación de Control Interno.

2. **Evaluación del riesgo:** su propósito es identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales.

3. **Actividades de control:** su propósito es permitir el control de los riesgos identificados y como mecanismo para apalancar el logro de los objetivos y forma parte integral de los procesos.

4. **Información y comunicación:** tiene como propósito utilizar la información de manera adecuada y comunicarla por los medios y en los tiempos oportunos. Para su desarrollo se deben diseñar políticas, directrices y mecanismos de consecución, captura, procesamiento y generación de datos dentro y en el entorno de cada entidad, que satisfagan la necesidad d de divulgar los resultados, de mostrar mejoras en la gestión administrativa y procurar que la información y la comunicación de la entidad y de cada proceso sea adecuada a las necesidades específicas de los grupos de valor y grupos de interés.

5. **Actividades de monitoreo:** su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como evaluaciones periódicas (autoevaluación, auditorías) que permiten valorar: (i) la efectividad del control interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública. (…)”

**En cuanto al esquema de líneas de defensa se define lo siguiente:**

- **Línea estratégica de defensa:** está conformada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno. La responsabilidad de esta línea de defensa se centra 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.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	26 de 52

- ✓ Primera línea de defensa: esta línea de defensa les corresponde a los servidores en sus diferentes niveles, quienes aplican 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.
- ✓ Segunda línea de defensa: esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

Aquí se incluyen a los jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de cada organización. Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica)

Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.

Entre los parámetros a tener en cuenta, para definir esta línea son los siguientes:

- Pertener a la media o alta gerencia:  
Dentro del Organigrama aquellos cargos que dependen del Representante Legal (Alta Gerencia), Para Media Gerencia, aquellos que se desprenden de los cargos anteriormente mencionados.
  - Responder ante la Alta Dirección: Aquel cargo que maneja un tema transversal para toda la entidad y responde ante el Representante Legal.
  - Evaluar y efectuar seguimiento a los controles aplicados por la 1ª línea de defensa.
- ✓ Tercera línea de defensa: esta línea de defensa está conformada por la Oficina de Control Interno, quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos o inadecuadamente cubiertos por la 2ª línea de defensa. La interacción entre la 2ª línea de defensa (proveedores internos de aseguramiento) y la 3ª línea de defensa y estas con los proveedores externos de aseguramiento (organismos de control y otras instancias de supervisión o vigilancia) serán representadas en una matriz de doble entrada denominada mapa de aseguramiento<sup>8</sup>, herramienta considerada por el Instituto de

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	27 de 52

Audidores como adecuada e idónea para coordinar las diferentes actividades de aseguramiento, visualizar el esfuerzo en común y mitigar los riesgos de una manera mucho más integral. (...)"

Luego entonces, la Línea Estratégica debe definir lineamientos claros frente a la estructura de control, por lo que específicamente a través del componente Ambiente de Control debe generar los espacios para el análisis y seguimiento de 63 los temas relacionados con el Talento Humano, la Integridad y la Planeación Estratégica, claves para que se cuente con ambiente propicio o favorable al control. De igual forma, a través de los demás componentes del MECI, podrá tomar decisiones basados en hechos y datos, ya que los miembros de 2ª línea que se identifiquen aportarán información a tiempo, con evaluaciones en términos de control y riesgos, lo que facilitará tomar acciones que eviten situaciones no deseadas en la entidad en tiempo real.

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.

Dentro de esta 2ª línea se encuentran la Oficina Asesora de Planeación o quien haga sus veces quienes lideran temas estratégicos para la entidad, como sería el seguimiento a la planeación institucional y a la gestión del riesgo; así mismo, se deberán incluir otras instancias internas que lideren temas estratégicos y transversales relacionados con planes, programas y/o proyectos fundamentales para el cumplimiento misional, así como otras instancias de apoyo que son transversales y garantizan el manejo de los recursos y bienes de la entidad.

Por último, la 3ª línea de defensa la conforma la Oficina de Control Interno o quien haga sus veces en la entidad, quien, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna se pronuncian sobre la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en cumplimiento de su rol de enfoque hacia la prevención se articulan con la oficina de planeación o quien haga sus veces, así como con las demás instancias de 2ª línea que se identifiquen, para compartir información y análisis de contraste que permita monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo o de forma integral.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

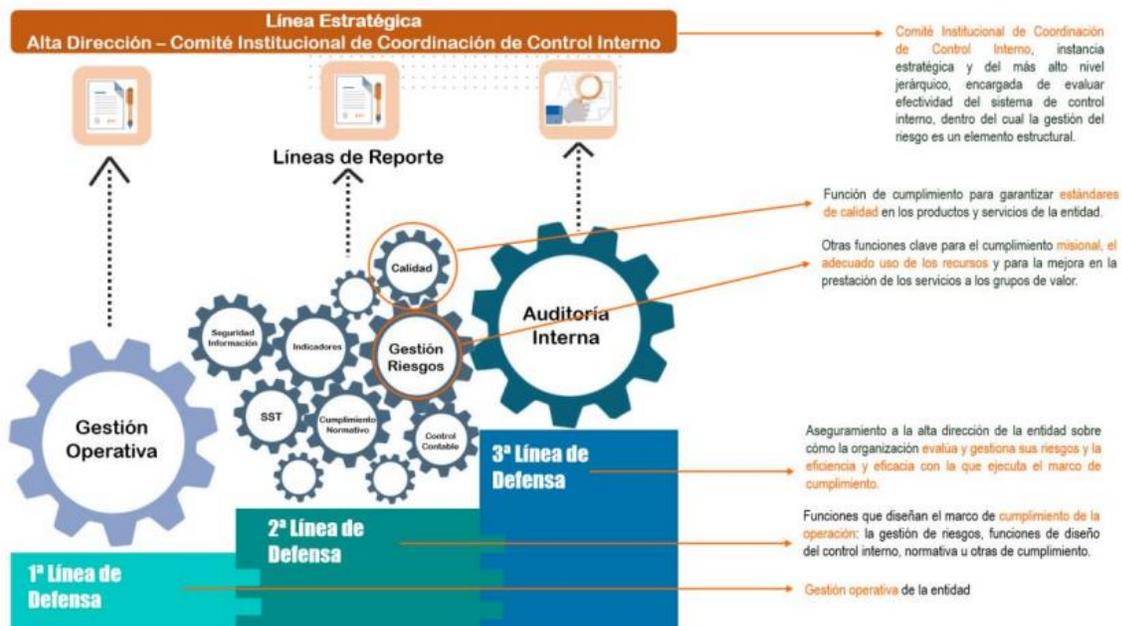


Ilustración 4 Operatividad Esquema de líneas de defensa  
Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

<b>Elaboro</b> Profesional SIG	<b>Reviso</b> Profesional SIG	<b>Aprobó</b> Profesional SIG
-----------------------------------	----------------------------------	----------------------------------

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	29 de 52

## 5. Lineamientos para el análisis del control fiscal

### 5.1 Control fiscal interno y prevención del riesgo fiscal:

la construcción de este capítulo tiene 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 (Decreto 403, 2020, art.6).

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. Para tener claro el ámbito normativo y jurídico, es necesario precisar que sus bases están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, los cuales fueron modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública

A partir de lo anterior, el control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno, con lo cual surgen conceptos clave como:

- Control fiscal Multinivel: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación del control social.

Control fiscal Interno (CFI): Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales s de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

En el nuevo modelo constitucional el control externo adquiere un enfoque preventivo y a su vez el control interno potencia el enfoque preventivo, partiendo de la premisa de que el Sistema de Control Interno es fundamental para conjugar el logro de resultados, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labor es de cobro, entre otros), a través de la prevención de responsabilidades.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	30 de 52

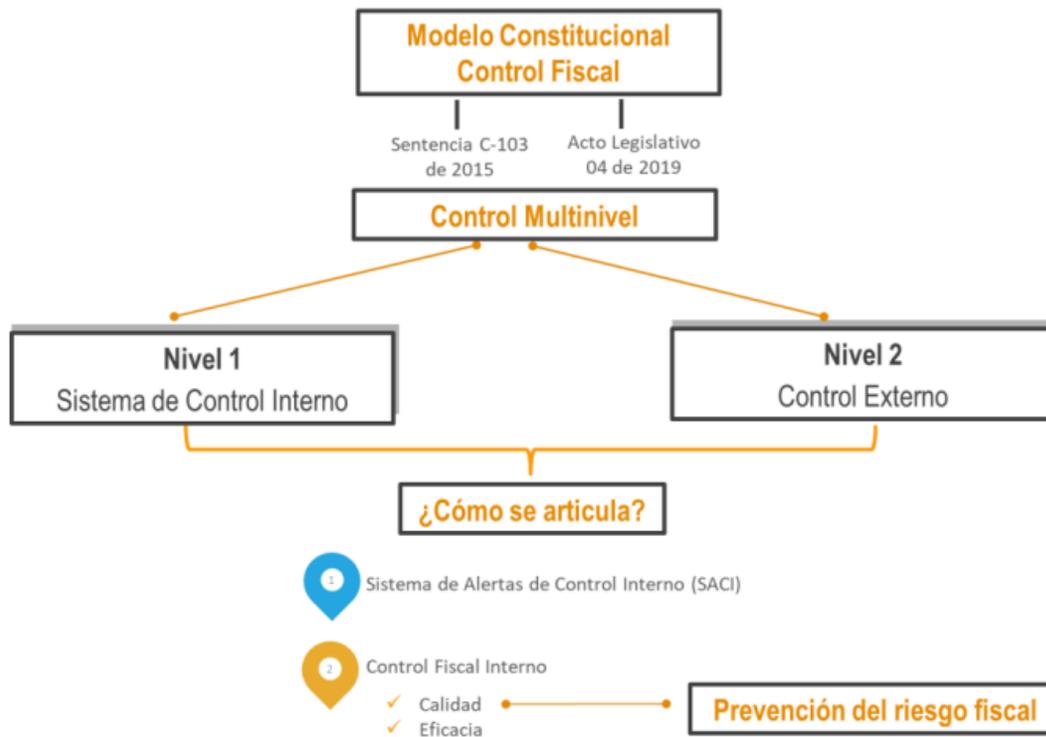


Ilustración 5 Articulación modelo constitucional control fiscal y sistema de control interno  
Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 20 22.

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

La metodología que se propone es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite, mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos.

## 5.2 Definición y elementos del riesgo fiscal:

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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

**Efecto:** es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	31 de 52

**Evento Potencial:** Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.

En esta guía, el evento potencial es equivalente a la causa raíz. Lo anterior se puede resumir de la siguiente manera:

<b>Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso</b>
--

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.

### 5.3 Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales:

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, que es fundamental para el resultado de la gestión de cada entidad y para la seguridad y prevención de responsabilidades de los gestores públicos (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros).

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

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Ahora bien, para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	32 de 52

gestión fiscal en las que potencialmente se genera riesgo fiscal) y circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal). Para este taller, puede usar las siguientes preguntas orientadoras:

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	<p>¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).</p>
Puntos de riesgo fiscal y circunstancias inmediatas	<p>Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-.</p> <p><b>Nota 1:</b> Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.</p> <p><b>Nota 2:</b> Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.</p> <p><b>Nota 3:</b> Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañinos sobre los recursos, bienes o intereses patrimoniales del Estado.</p> <p><b>Nota 4:</b> La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.</p>

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	33 de 52

Sirve para identificar	Preguntas y respuestas para la identificación
Circunstancias inmediatas	<p>En un ejercicio autocrítico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años?</p> <p><b>Nota:</b> Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.</p>
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del “¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” (anexo1), son aplicables a la entidad?

*Ilustración 6 Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas*  
Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

#### 5.4 Identificación de las áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo. Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- ✓ Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones
- ✓ Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo uno de conceptos básicos).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos ; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública (consultar definiciones en el capítulo uno de conceptos básicos ).

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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	34 de 52

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio esta tal

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador- causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto- (Contraloría General de la República, 2021).

Ejemplo: Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por \$30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

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

**¿Cuál es el hecho generador?** La omisión de pagó oportuno del canon de arrendamiento. Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

### 5.5 descripción del riesgo fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

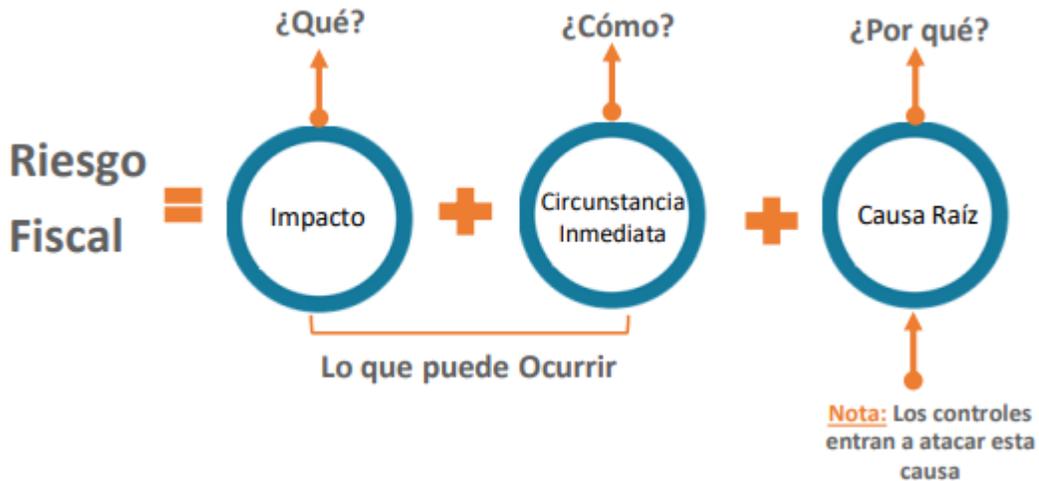
Para redactar un riesgo fiscal se debe tener en cuenta:

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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	35 de 52

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



Ejemplo:

**Proceso: Gestión de Recursos**

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

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



¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre <b>bienes públicos</b>	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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA	<b>GUIA ADMINISTRACION DE RIESGOS DE          GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	36 de 52

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública.

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

*Ilustración 7 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso  
 Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.*

## 5.6 Paso 2: Valoración del riesgo fiscal

**Evaluación de riesgos** Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

**Probabilidad** La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal. Teniendo esto de presente, para definir el nivel de probabilidad, se ha de tener en cuenta la siguiente tabla definida en el numeral 3.1 de la presente guía:

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <b>UMAYOR</b> INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA	<b>GUIA ADMINISTRACION DE RIESGOS DE          GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	37 de 52

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

Nota: Es necesario mencionar, que las frecuencias pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que las frecuencias en cada nivel pueden ser adaptadas a las necesidades y complejidad de cada entidad.

- **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, se aplicará la siguiente tabla definida en el numeral 3.1 de la presente guía:

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	38 de 52

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

**Nota:** Es necesario mencionar, que los niveles en la afectación económica pueden variar según el tamaño y complejidad de los procesos de la entidad, así como sus necesidades, por lo que los rangos en cada nivel pueden ser adaptados a las necesidades y complejidad de cada entidad

- **Determinación del nivel de riesgo inherente**

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad, para lo cual se aplica la matriz definida en el numeral 3.2 de la presente guía:

		Impacto												
Probabilidad		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%								
	Muy Alta 100%						Extremo	Alto	Moderado	Bajo				
	Alta 80%													
	Media 60%													
	Baja 40%													
	Muy Baja 20%													

**Nota:** Es necesario mencionar, que esta matriz de severidad está diseñada de acuerdo con estándares internacionales que permiten tener trazabilidad en los desplazamientos en cada zona, por lo que se recomienda no modificarla.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	39 de 52

### 5.7 Valoración de los controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

#### Tipologías de controles:

- ✓ 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 fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- ✓ Control Detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- ✓ 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

### 6. Riesgos de corrupción

Definición de riesgo de corrupción: Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

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

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

**ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.**

Los riesgos de corrupción se establecen sobre procesos.

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

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	40 de 52

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

### 6.1 Generalidades acerca de los riesgos de corrupción

- ✓ Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.
- ✓ Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.
- ✓ Consolidación: la oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.
- ✓ Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- ✓ Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, o la de gestión del riesgo deberá

Elaboro	Reviso	Aprobó
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	41 de 52

diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción.

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados

- Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.
- 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 de corrupción.
- Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

## EJEMPLO

Información anonimizada:

N.º	Riesgo	Clasificación	Causa	Probabilidad	Impacto	Riesgo Residual	Opción de Manejo	Actividad de Control
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros...	Corrupción	Falta de...	Probable	Catastrófico	Catastrófico	Evitar	[Redacted]

Información anonimizada

### ¡IMPORTANTE

Tenga en cuenta que la información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.

Una resolución no puede calificar la información como clasificada o reservada.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	42 de 52

## IMPORTANTE

Los riesgos de corrupción, siempre deben gestionarse.

**IMPORTANTE**

En la descripción de los riesgos de corrupción deben concurrir **TODOS** los componentes de su definición:

**Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.**

Fuente: Secretaría de Transparencia de la Presidencia de la República

### Valoración de riesgos

#### Cálculo de la probabilidad e impacto

#### Análisis de la probabilidad

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

Criterios para calificar la probabilidad.

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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	43 de 52

## 6.2 Análisis del impacto

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

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.		<b>10</b>	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

**Nivel de  
impacto  
MAYOR**

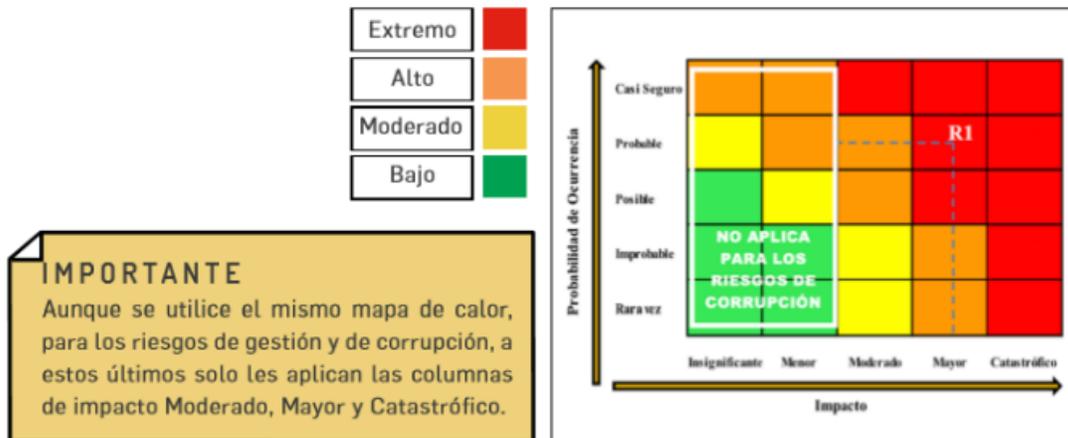
<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	44 de 52

### 6.3 Análisis del impacto en riesgos de corrupción

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

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



### 6.4 Valoración de los controles – diseño de controles

Tenga en cuenta para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, por lo tanto, se sugiere remitirse a dicho documento.

Nivel del riesgo (riesgo residual)

Desplazamiento del riesgo inherente para calcular el riesgo residual.

### 6.5 Tratamiento del riesgo

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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	45 de 52



Ilustración 8 Tratamiento del riesgo  
Fuente: DAFP

### 6.6 Aceptar el riesgo

**IMPORTANTE**  
En el caso de riesgos de corrupción, estos no pueden ser aceptados.

### 6.7 evitar el riesgo

Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

**6.8 compartir el riesgo** Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	46 de 52

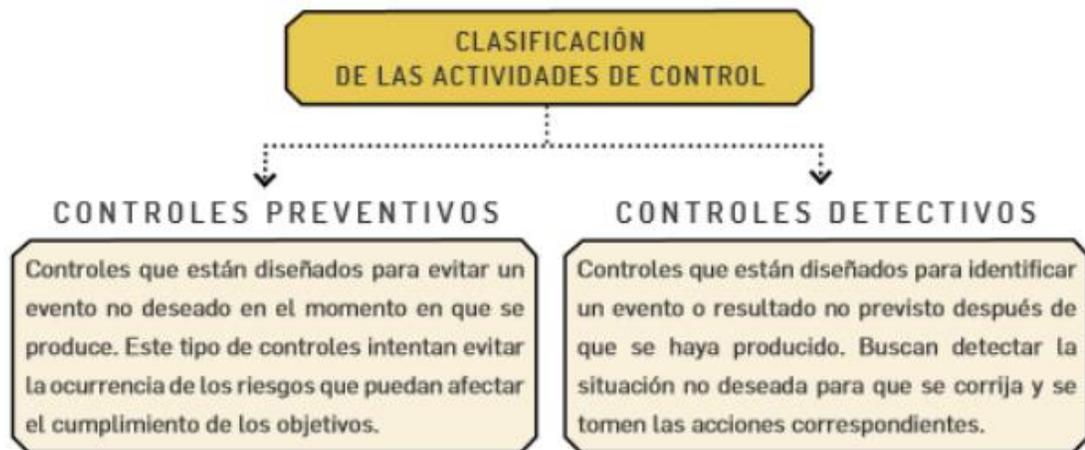
parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

**6.8 Reducir el riesgo** El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

### 6.9 Tratamiento del riesgo

- Rol de la primera línea de defensa Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.



**6.9.1 Monitoreo de riesgos de corrupción** Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	47 de 52

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

### **Reporte de la gestión del riesgo de corrupción**

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

### **Seguimiento de riesgos de corrupción**

#### **GESTION RIESGOS DE CORRUPCIÓN**

- Seguimiento: El jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.
- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtir dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtir dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtir dentro de los diez (10) primeros días del mes de enero. El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. (Ver anexo 6. matriz de seguimiento a los riesgos de corrupción) En especial deberá adelantar las siguientes actividades:
  - ✓ Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
  - ✓ Seguimiento a la gestión del riesgo.
  - ✓ Revisión de los riesgos y su evolución.
  - ✓ Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

### **Acciones a seguir en caso de materialización de riesgos de corrupción**

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

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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <p>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</p>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	48 de 52

4) Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

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

**7. Lineamientos seguridad de la información**

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

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

¿Qué son los activos?	¿Por qué identificar los activos?
<p>Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:</p> <p>-Aplicaciones de la organización</p>	<p>Permite determinar <b>qué es lo más importante que cada entidad y sus procesos poseen</b> (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).</p>

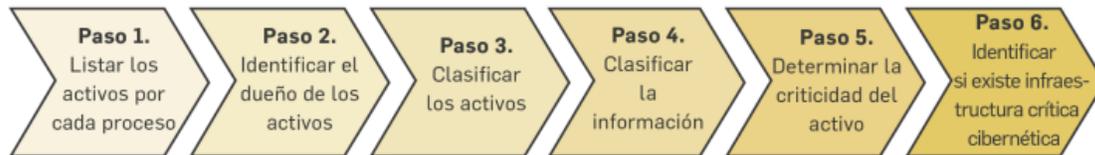
<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	49 de 52

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber <b>qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano,</b> aumentando así su confianza en el uso del entorno digital.

*Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020*

### ¿CÓMO IDENTIFICAR LOS ACTIVOS?:



**Nota:** para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas” que hace parte de los anexos de la presente guía.

**7.2 Identificación del riesgo:** se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el 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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	50 de 52

**Nota:** 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.

**IMPORTANTE**

- \* Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- \* Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas", el cual hace parte de la presente guía.
- \* **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- \* **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

### 7.3 Valoración del riesgo:

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía. En este sentido, se debe considerar para este análisis la tabla 4 definida en el aparte 3.1.1, la cual se retoma a continuación:

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

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <b>UMAYOR</b> INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA	<b>GUIA ADMINISTRACION DE RIESGOS DE          GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	51 de 52

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 de la presente guía, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

#### 7.4 Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en el documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la pérdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Ilustración 9: Controles para riesgos de seguridad de la información  
 Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG

 <b>INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA</b>	<b>GUIA ADMINISTRACION DE RIESGOS DE GESTIÓN Y OPORTUNIDADES</b>	Código	GI-SM-001
		Versión	2
		Fecha	23/08/2024
		Página	52 de 52

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	<b>Pérdida de la integridad</b>	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	<b>EFICACIA:</b> Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100  <b>EFFECTIVIDAD:</b> Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
				Contraसेñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018		
				Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018		
				"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018		

Ilustración 10 Formato mapa riesgos seguridad de la información

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

## 8. CONTROL DE MODIFICACIONES

CONTROL DE CAMBIOS			
Versión	Fecha	Descripción del cambio	Responsable Aprobación
0	25/03/2020	Elaboración del documento	Director de Planeación y Mejoramiento de la calidad
1	7/09/2020	Modificación de sección 4.	Director de Planeación y Mejoramiento de la calidad
2	23/08/2024	Inclusión de los riesgos fiscales, guía administración del riesgo V6	Profesional sig.

<b>Elaboro</b>	<b>Reviso</b>	<b>Aprobó</b>
Profesional SIG	Profesional SIG	Profesional SIG