Contenido

1.OBJETIVO GUÍA

Establecer el marco general para la gestión del riesgo en todos los niveles de la entidad, abarcando las diferentes metodologías dispuestas para el desarrollo de la identificación y tratamiento para riesgos de gestión, fiscales, corrupción, Fraude, soborno, sarlaft, seguridad y salud en el trabajo, Seguridad de la información (Sistema de Gestión de Riesgos para la Integridad Pública SIGRIP) y continuidad del negocio que afecten el cumplimiento de la misionalidad y el logro de sus objetivos institucionales y de los sistemas de gestión

2 SISTEMA INTEGRADO DE GESTIÓN DEL RIESGO INSTITUCIONAL (SIGRIP)

La metodología para los riesgos SIGRIP se realiza bajo los lineamientos definidos por el Departamento Administrativo de la Función Pública - Guía para la gestión Integral del riesgo en entidades públicas versión 7 de agosto de 2025.

2.1 Metodología riesgos SIGRIP

Sistema articulado que integra la gestión de riesgos de gestión, corrupción, fraude y seguridad y salud en el trabajo, bajo un enfoque preventivo, alineado con MIPG y la Guía de la Función Pública DAFP V7.

Actualmente la Secretaria Distrital de Movilidad SDM maneja metodologías separadas establecidas de acuerdo a la versión 4 donde se articulan las políticas de lucha contra la corrupción y seguridad de la información, la versión 6 donde se incorpora el riesgos fiscal y GTC 45. Con la nueva versión 7 el SIGRIP plantea la integración en un solo ciclo metodológico y se establece un modelo único aplicable a todos los tipos de riesgo:

- Riesgos de gestión
- Riesgos de corrupción / fraude / Conflictos de interés
- Riesgos de soborno
- Riesgos de lavado de activos
- Riesgos fiscales
- Riesgos SST

Figura 1 Metodología Política SIGRIP

2.2 Identificación del Riesgo

La identificación del riesgo en el marco del Sistema de Gestión de Riesgo para la Integridad Pública (SIGRIP) constituye una fase fundamental orientada a reconocer, describir y documentar de manera estructurada los eventos potenciales que puedan afectar el cumplimiento de los objetivos institucionales, la prestación del servicio, la integridad de los recursos públicos y la confianza ciudadana.

Este proceso se desarrolla bajo un enfoque preventivo, sistemático e integral, que permite la identificación unificada de los diferentes tipos de riesgo, incluyendo riesgos de gestión, corrupción, fraude, fiscales y de seguridad y salud en el trabajo, evitando la fragmentación metodológica y garantizando la trazabilidad institucional.

La identificación de riesgos se realiza a partir del análisis del contexto organizacional previamente definido, considerando tanto factores internos como externos, así como la revisión detallada de los procesos, procedimientos, actividades críticas, puntos de control, interacciones con terceros y escenarios de vulnerabilidad.

Los líderes de proceso, con el acompañamiento de la Oficina Asesora de Planeación, deberán identificar los riesgos asociados a sus procesos, teniendo en cuenta, entre otros, los siguientes aspectos:

- Objetivos del proceso y su alineación con el direccionamiento estratégico institucional
- Actividades críticas o sensibles
- Puntos de decisión con discrecionalidad
- Interacción con ciudadanos, contratistas y otras partes interesadas
- Manejo de recursos financieros, información o bienes públicos
- Antecedentes de eventos materializados o hallazgos de control
- Riesgos emergentes derivados de cambios normativos, tecnológicos o del entorno

Todos los riesgos identificados deberán registrarse en la **matriz de riesgos SIGRIP**, garantizando consistencia en la información, evitando duplicidades y permitiendo su posterior análisis, evaluación y tratamiento dentro de un modelo integrado.

3. RIESGOS DE GESTIÓN

3.1 Metodología riesgos de gestión

La metodología para los riesgos de Gestión se realizan bajo los lineamientos definidos por el Departamento Administrativo de la Función Pública - Guía para la gestión Integral del riesgo en entidades públicas versión 7 de agosto de 2025.

3.2 Identificación del riesgo

La identificación es la etapa donde se analizan los riesgos que están bajo el control de la organización, para la cual se debe tener en cuenta el contexto estratégico en el que opera la entidad, de igual manera el análisis de los factores internos y externos que afecten el cumplimiento de los objetivos institucionales.

a. Análisis de objetivos estratégicos y de los procesos:

Análisis de objetivos estratégicos	Análisis de objetivos del proceso
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso	Los objetivos de los procesos deben estar alineados con los objetivos estratégicos, así como de su misión y visión

Cadena de valor

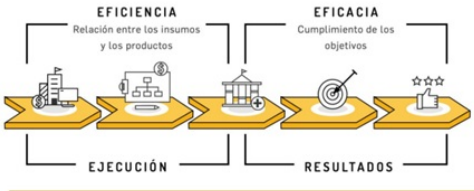


Figura 2 Cadena de valor

Por medio de la cadena de valor se pueden identificar las actividades que están dentro del flujo del proceso y a partir de éstas identificar la posibilidad de presentarse la materialización de un riesgo en el cumplimento de los objetivos del proceso o de la entidad.

b. **Área de impacto**

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional, para algunos riesgos puede presentarse que la afectación sea de tipo económica y reputacional a la vez.

c. **Descripción del riesgo**

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

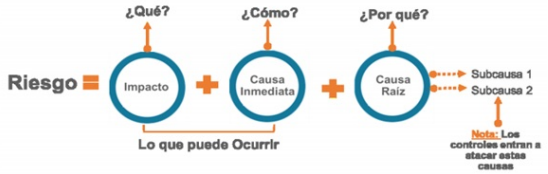


Figura 3 Redacción del riesgo

Ejemplo:

Proceso: gestión de recursos

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

Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisidores) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas. Atendiendo el esquema propuesto para la redacción del riesgo, se tiene:

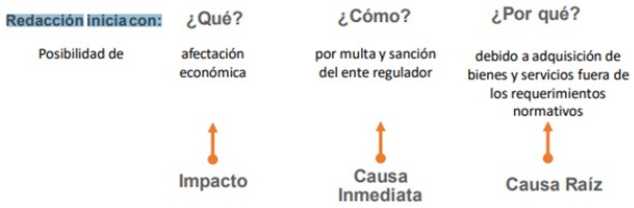


Figura 4 Ejemplo redacción del riesgo

Redacción final del riesgo: Afectación económica por multa y sanción del ente regulador debido a adquisición de bienes y servicios fuera de los requerimientos normativos.

Premisas para una adecuada redacción del riesgo:

- No describir como riesgos omisiones o desviaciones del control.
- No describir causas como riesgos
- No describir riesgos como la negación de un control
- No existen riesgos transversales, lo que pueden existir son causas transversales.

d. Clasificación del riesgo

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

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

Figura 5 Cuadro clasificación del riesgo

Figura 6 Relación entre factores de riesgo y la clasificación

Una vez se tenga toda la información, se tiene la primera parte para la construcción del mapa de riesgos en su etapa de identificación.

Figura 7 Primera parte construcción mapa de riesgos

3.3 Valoración del riesgo

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

a. Tabla de probabilidad: Teniendo en cuenta el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, la cual se describe en la siguiente tabla, que establece los criterios para definir el nivel de probabilidad.

	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%

Figura 8 Tabla de probabilidad

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

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

Figura 9 Tabla de impacto

Frente al análisis de probabilidad e impacto no se utiliza el criterio experto, esto quiere decir que el líder del proceso, como conocedor de su que hacer, defina cuantas veces desarrolla la actividad.

Ejemplo (continuación):

Proceso: gestión de recursos

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

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

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

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

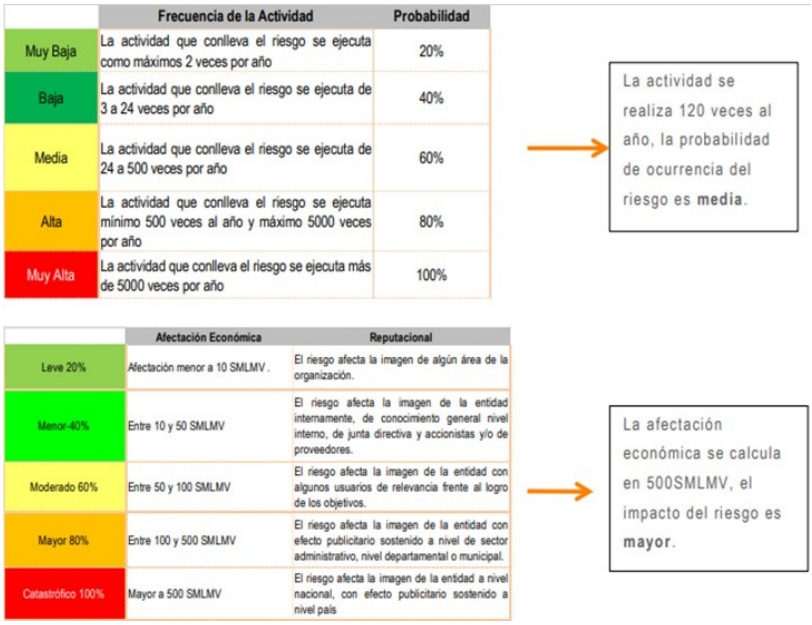


Figura 10 Tabla resumen ejemplo

3.4 Evaluación del riesgo

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

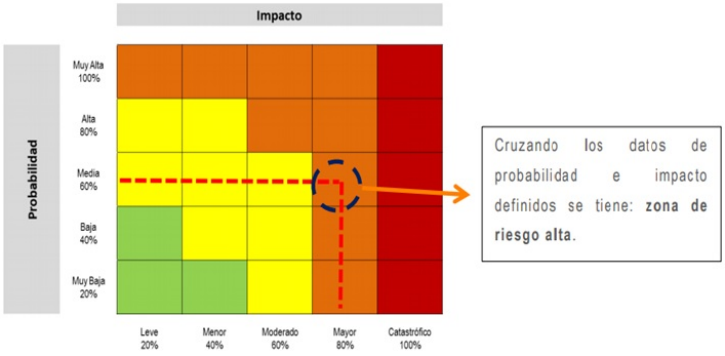


Figura 11 Mapa de calor

3.5 Valoración de controles

Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con las/los líderes de procesos o colaboradoras y colaboradores expertos en su qué hacer. En este caso si aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son las/los líderes de proceso con el apoyo de su equipo de trabajo
- Estructura para la descripción del control: Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:
- Responsable de ejecutar el control: Identifica el cargo de la/el servidor (a) 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.

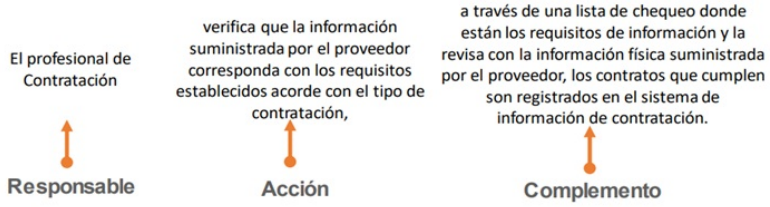


Figura 12 Ejemplo redacción del control

3.6 Tipología de controles

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

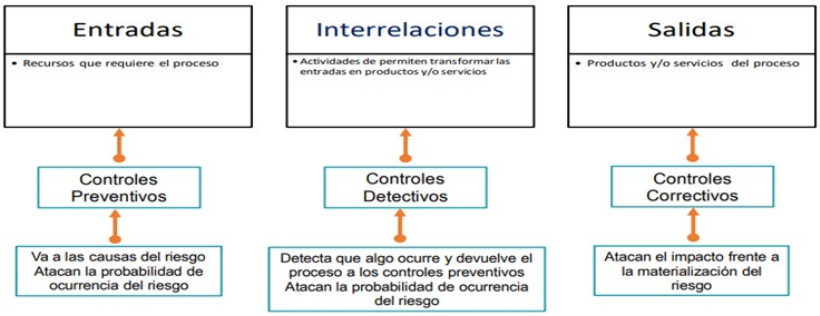


Figura 13 Ciclo del proceso y las tipologías de los controles

- 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.

De igual manera de la forma como se ejecutan los controles se tiene:

- Control manual: Son ejecutados por personas
- Control automático: Ejecutados por un sistema

3.7 Análisis y evaluación de controles

A continuación, se analizan los atributos del control entre atributos de eficiencia y atributos de documentación.

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

Figura 14 Tabla de atributos

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que del valor de los atributos se genera el movimiento del mapa de calor, se debe tener en cuenta los tipos de movimientos dependiendo del tipo de control implementado.

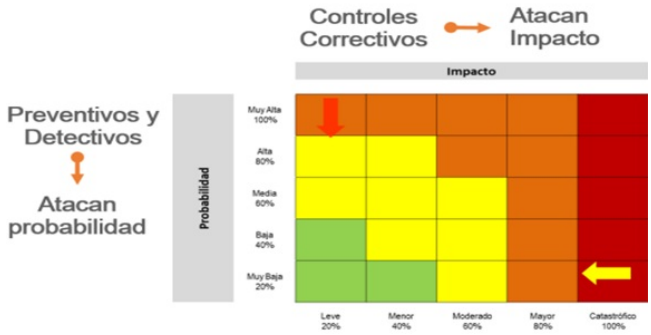


Figura 15 Movimientos en el mapa de calor

Ejemplo:

Proceso: gestión de recursos

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

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

Probabilidad Inherente= moderada 60%

Impacto Inherente: mayor 80%

Zona de riesgo: alta

Controles identificados:

Control 1: La/el profesional del área de contratos 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, 48 los contratos que cumplen son registrados en el sistema de información de contratación.

Control 2: La/el jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Aplicación de atributos según la información del ejemplo:

Controles y sus características				Peso
Control 1 El profesional del área de contratos 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, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con registro	X	-
		Sin registro		-
Total valoración control 1				**40%**

Figura 16 Evaluación control

Como se observa se evalua en el control 1 los atributos en cuanto al tipo de control (preventivo) con valor de 25% y su implementación (manual) con valor de 15%, dando un total de 40

De la misma manera se hace para el control 2, teniendo un valor de 30% con el mismo analisis del control anterior.

3.8 Nivel de riesgo residual

Con esta información se procede a realizar el calculo del nivel de riesgo residual de la siguiente manera.

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

Figura 17 Evaluación riesgo residual

Acorde a la información de cada control y su valoración en los atributos, se procede a realizar una operación con la siguiente información:

- Valor de probabilidad antes de controles.
- Valor de atributos del primer control

Del resultado de la multiplicación de ambos se obtiene el porcentaje que se le resta a la probabilidad inicial, lo cual indica el porcentaje de reducción en probabilidad.

Valor de probabilidad antes de controles: 60%

Valor de atributos del control 1: 40%

60%*40% = 24%

Este último lo restamos al valor incial de probabilidad

60% - 24% = 36%

Como para el ejemplo se tenían dos controles se toma el valor resultado del primero y de la misma manera se calcula frente al valor de probabilidad y el valor del control. Esto indica que dependerá del numero de controles el total de dismunición en probabilidad.

Se inicia con el ultimo valor de probabilidad dado (36%)

36%*30% = 10.8%

Nuevamente se resta del último valor de probabilidad que es 36%

36% - 10.8% = 25.2%

Teniendo como resultado final para probabilidad la nueva ubicación en el mapa de calor en un porcentaje de probabilidad de 25.2%

Para los movimientos de impacto se realizan de la misma manera teniendo como referencia no la probabilidad inicial, sino el impacto inicial.

En la siguiente tabla se encuentra un resumen del ejercicio de ejemplo hasta la valoración del riesgo ineherente.

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

Referencia	Impacto	Causa inmediata	Causa raiz	Descripción del riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente
1	Afectación económica	Multa y sanción del organismo de control	Incumplimiento de los requisitos para contratación	Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos.	Ejecución y administración de procesos	120	Moderada	60%	Mayor	80%	Alta

Figura 18 Mapa de riesgos valoración del riesgo inherente

A continuación se aprecia la evaluación del control del ejemplo dentro del mapa de riesgos y su comportamiento en el mapa de calor, teniendo como resultado un nivel de riesgo residual alto para el primer control.

No. control	Descripción del control	Afectación		Atributos						Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
1	El profesional del área de contratos 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, los contratos que cumplen son registrados en el sistema de información de contratación.	X		Preventivo	Manual	40%	Documentado	Continua	Registro material	36%	Baja	25,2%	Mayor	80%	Alta	Reducir

Figura 19 Mapa de riesgos valoración del residual

3.9 Estrategias para combatir el riesgo

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

Figura 20 Política de tratamiento del riesgo residual

Para la política de tratamiento Reducir mitigar se genera un plan de acción, el cual debe ser diferente a los controles y su intensión será la de mitigar el riesgo como tal.

Ejemplo:

Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

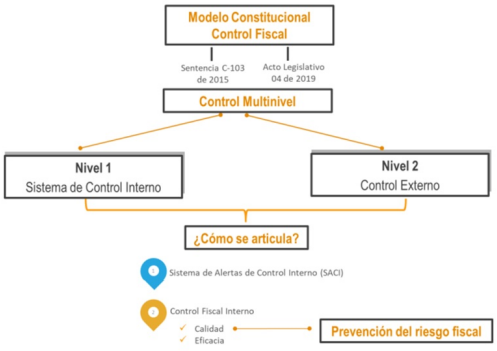
Figura 21 Plan de acción ejemplo

3.10 Lineamientos para la gestión de los riesgos de tipo fiscal

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

Para la identificación, valoración y diseño de controles para los riesgos de tipo fiscal es indispensable tener en cuenta el catálogo indicativo de puntos de riesgos fiscal y circunstancias inmediatas. por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública y que potencialmente pueden generar un efecto dañoso al patrimonio público

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.



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Figura 22 Modelo Riesgo Tipo Fiscal

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

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

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.

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.

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

Lo anterior se puede resumir de la siguiente manera:

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

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

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

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).

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 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	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: 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. Nota 3: 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 dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: 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.
Circunstancias inmediatas	En un ejercicio autocritico, 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? Nota: 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.
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" son aplicables a la entidad?

Identificación de áreas de impacto:

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

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

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

1. Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.
2. 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).

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.

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 efi ciente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

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

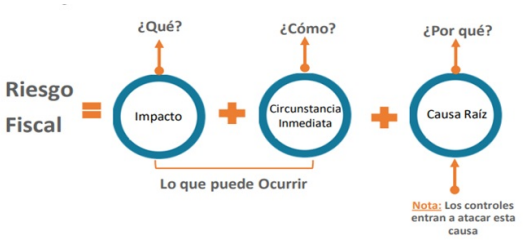


Figura 23 Estructura redacción Riesgos Fiscales

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 **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Figura 24 Redacción Riesgos Fiscales

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

Figura 25 Efectos Fiscales

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

Para el ejercicio de análisis de probabilidad se utiliza el mismo utilizado para los riesgos de gestión.

Impacto: Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendra 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 la metodología de riesgos de gestión.

En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de $2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico

La valoración y el diseño de controles de igual manera se realizan teniendo en cuenta los lineamientos para los riesgos de gestión.

La evaluación del control se realiza de la siguiente manera:

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

23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratistas
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o

		coactivo) o judicial

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2022

Lineamientos institucionales para la gestión de los riesgos de gestión:

1. Para la adecuada identificación de los riesgos, los procesos deben analizar las actividades que realizan conforme a su caracterización, con el fin de tener una mayor cobertura de los posibles eventos de riesgos al que esta expuesto el proceso.

2. Para poder determinar el uso de los controles, es necesario tener en cuenta:

a) Para los riesgos de gestión solo aplican los controles de tipo Correctivo, Preventivo y Detectivo

b) Los controles de tipo de correptivo deben garantizar que realmente corriga el evento materializado

c) Las definiciones son las siguientes:

- **Control**: Medida que permite reducir o mitigar un riesgo.
- **Controles Preventivos** (Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo)
- **Controles Detectivos** (Detecta que algo ocurre y devuelve el proceso a los controles preventivos Atacan la probabilidad de ocurrencia del riesgo)
- **Controles Correctivos** (Atacan el impacto frente a la materialización del riesgo)

4 RIESGOS DE CORRUPCIÓN, FRAUDE Y CONFLICTOS DE INTERÉS

La metodología para los riesgos de corrupción y Fraude se realizan bajo los lineamientos definidos por el Departamento Administrativo de la Función Pública - Guía para la gestión Integral del riesgo en entidades públicas versión 7 de agosto de 2025.

4.1 Metodologia de Gestión Riesgos de Corrupción, Fraude y Conflictos de interés

El riesgo de corrupción se define como todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. 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.

Dado el nuevo esquema SIGRIP los riesgos de corrupción se actualizan dentro del mismo ciclo integral de riesgos, no como sistema independiente esto implica que tendrán la misma metodología, matriz, y análisis (pero con tratamiento diferencial).

4.2 Identificación del riesgo de corrupción, fraude y conflictos de interés

Dentro del proceso de identificación del riesgo se debe tener presente que este debe estar alineado a los estándares de la entidad como es la misión, visión y objetivos estratégicos y deben contener los atributos SMART donde deben ser específicos, medibles, alcanzables, realistas y con un tiempo de ejecución.

Los factores de Riesgo son las fuentes generadoras de riesgos que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa e incrementan el nivel de exposición. Se deben tener presente factores de riesgo que pueden incidir en los procesos como puede ser:

- Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.
- Eventos por situaciones externas que afectan la entidad.

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

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

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

Figura 26 Matriz de definición del riesgo

Para la identificación de los riesgos se deben considerar los siguientes componentes y principios:

- **Gobierno y Cultura:** Base para los componentes de la gestión del riesgo reforzando su importancia y estableciendo responsabilidades de supervisión al respecto
- **Establecimiento de la estrategia y objetivos**: La gestión del riesgo se integra en el plan estratégico de la entidad a través del proceso de analisis del contexto interno y externo, definición del apetito del riesgo, evaluación de las estrategias alternativas y formula objetivos estratégicos y operacionales.
- **Desempeño**: Identifica y evalúa los riesgos que pueden afectar la capacidad de la SDM para alcanzar la plataforma y los objetivos estratégicos.
- **Revisión y Monitoreo**: Examina las capacidades y técnicas de gestión del riesgop y el desempeño de la entidad en relación con los objetivos.
- **Información, Comunicación y Reporte**: Proceso continuo e iterativo de obtener y compartir información en toda la entidad.

Descripción del Riesgo

Dentro del proceso de descripción del riesgo se debe tener en cuenta que iniciaría con la formulación “Posibilidad de” señalando el Impacto refiriéndose a las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo. La causa inmediata son las circunstancias o situaciones específicas y claras más evidentes sobre las cuales se presenta el riesgo y de raíz que plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de los controles.

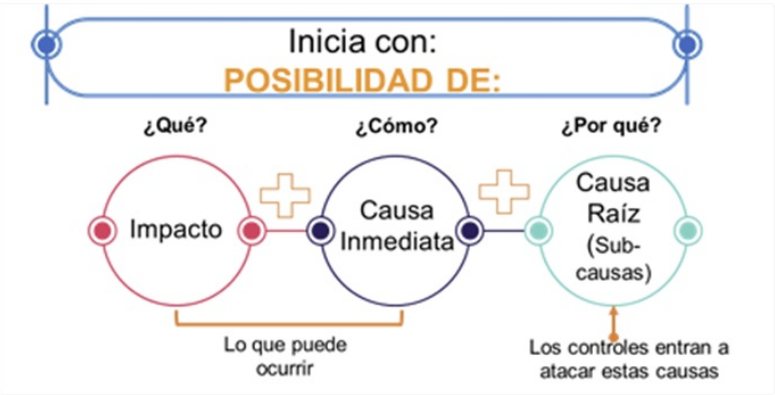


Figura 27 Estructura redacción del Riesgo

Ejemplo como referente para análisis del riesgo

Impacto	Causa Inmediata		Causa Raíz
Afectación económica y/o reputacional	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	Descripción de la actividad en el flujo del proceso

Al evento potencial se le asignan las posibles causas y consecuencias asociadas, se aclara que las causas y las consecuencias no son lineales, es decir por cada causa no necesariamente se requiere una consecuencia.

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

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

Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Clasificación del riesgo

Acorde a las siguientes tipologías se asocia el riesgo teniendo en cuenta lo relacionado en el siguiente cuadro.

TIPO	RIESGO	CONCEPTO
Riesgos asociados a la institucionalidad	Concentración de poder Extralimitación de funciones Ausencia o debilidad de procesos y procedimientos para la gestión administrativa y misional amiguismo y clientelismo Ausencia o debilidad de medidas y/o políticas de conflicto de interés Desvío de uso de los bienes y servicios de la entidad	Son generados por las conductas irregulares, deficientes en los procesos y procedimientos en la gestión institucional y por el aumento de la discrecionalidad en la toma de decisiones.
Riesgos asociados a la visibilidad de la gestión	Bajo nivel de publicidad de la información (transparencia activa) Rendición de cuentas a la ciudadanía de baja calidad (deficiente) Destrucción o alteración de información en los sistemas de información oficiales Falsedad en documento público Pérdida de documento público Ausencia de canales de comunicación	Son generados por la opacidad en la información, las restricciones para el acceso a información pública y bajo cumplimiento del principio de transparencia activa.
Riesgos asociados al control y sanción	Inexistencia de canales de denuncia interna y externa Bajos niveles de denuncia Bajos estándares éticos Baja cultura de control social Baja cultura de control institucional	Son los asociados a una baja cultura de auto regulación, control externo en la entidad y mecanismos de sanción por hechos de corrupción.
Riesgos asociados a delitos de la administación pública	Celebración indebida de contratos Peculado Tráfico de influencias Cohecho Concusión Enriquecimiento ilícito Prevaricato Concierto para delinquir Interés indebido en la celebración de contratos Abuso de autoridad por comisión de denuncia Utilización indebida de información oficial privilegiada Detrimento patrimonial malversación de recursos públicos	Se consideran estos riesgos asociados a posibles prácticas corruptas, delitos tipificados en las normas colombianas.

Figura 28 Tipologías de riesgos de corrupción

4.3 Valoración del riesgo Inherente

La valoración del riesgo inherente se realiza con base en las tablas de probabilidad e impacto, las cuales en conjunto evidencian el nivel de riesgo inherente para cada riesgo de corrupción identificado.

Determinar la Probabilidad:

Se entiende como la posibilidad de ocurrencia del riesgo, la probabilidad 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.

Con la aplicación de este esquema, se puede determinar con claridad la frecuencia con la que se lleva a cabo la actividad que genera la exposición al riesgo identificado y descrito, 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. La exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Figura 29 Nivel Probabilidad

Determinar el impacto:

Son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en versiones anteriores de la guía se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se hace necesario agruparlos en impacto económico y reputacional, con el fin de facilitar el análisis y evitar la subjetividad en los análisis por parte de los líderes internos.

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

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

Figura 30 Nivel de Impacto

Evaluación del nivel del Riesgo:

Se debe determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar el nivel de Riesgo Inherente.

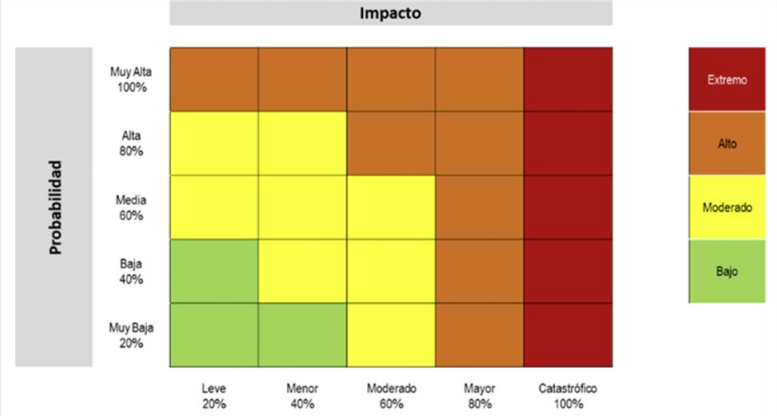


Figura 31 Matriz de Calor

De igual manera que con el riesgo de corrupción, se cuenta con un mapa de calor para el análisis de nivel de riesgo tanto inherente como residual, con la diferencia que este mapa no cuenta con niveles bajos, esto por su naturaleza de riesgo de corrupción no es tolerable un nivel de riesgo bajo.

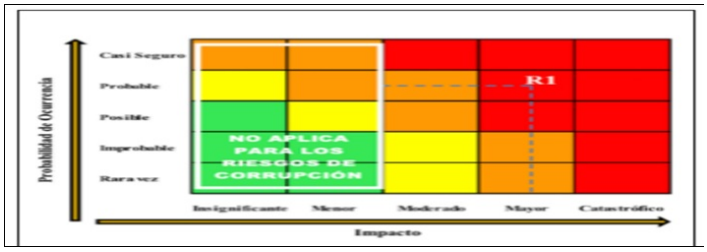


Figura 32 Zona aplicable para los riesgos de corrupción

Periodicidad de Seguimiento del Riesgo

Conforme a los lineamientos establecidos en la Guía de Riesgos versión 7, el seguimiento a los riesgos es una actividad esencial para garantizar su adecuada administración y la toma de decisiones oportunas por parte de la entidad. El seguimiento permite verificar la evolución de los riesgos identificados, identificar cambios en su nivel de probabilidad e impacto, y evaluar si las condiciones del contexto interno y externo han variado, pudiendo generar nuevos riesgos o modificar los existentes. De igual manera, facilita la detección temprana de la materialización de eventos de riesgo o de señales de alerta que requieran la implementación de acciones preventivas o correctivas.

4.4 Valoración de controles

La valoración de controles se realiza acorde con los parámetros señalados en la Guía de administración del riesgo y el diseño de controles en entidades públicas. En la estructuración de los controles asociados a los riesgos de corrupción y fraude, se debe considerar de manera integral la definición de la responsabilidad, las acciones y los complementos necesarios para su adecuada implementación y ejecución. Estos elementos permiten garantizar la efectividad del control y su correcta aplicación dentro de los procesos institucionales.

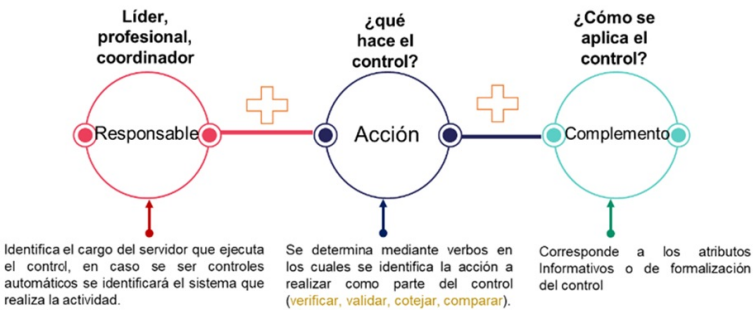


Figura 33 Redacción de controles

Para tal efecto, en la redacción de los controles se deben incorporar los siguientes atributos:

- **Responsable**: Corresponde al cargo del(os) servidor(es) público(s) encargado(s) de ejecutar el control (directivos, asesores, profesionales, técnicos o asistenciales). En el caso de controles automatizados, se deberá identificar el responsable de su calibración, parametrización y/o mantenimiento periódico dentro del sistema de información o software mediante el cual opera el control.
- **Acción**: Define el propósito del control, estableciendo claramente la actividad que se realiza. Se recomienda el uso de verbos que denoten actividades de verificación o aseguramiento, tales como: verificar, validar, conciliar, comparar, revisar, cotejar o detectar, con el fin de garantizar que los resultados obtenidos se ajusten a los objetivos definidos y a la normativa aplicable.
- **Complementos**: Comprenden los elementos adicionales que facilitan la implementación del control conforme a su diseño. Incluyen aspectos como la documentación de soporte, la frecuencia de ejecución, los registros generados y las condiciones específicas bajo las cuales debe desarrollarse el control.

En este sentido, la adecuada redacción debe integrar de manera coherente estos atributos, de modo que se constituyan en herramientas efectivas para la prevención, detección y mitigación de riesgos de corrupción, en concordancia con la estructura definida para la formulación de controles en la entidad.

4.5 Tipología del control

La metodología establece los siguientes tipos de atributos para los controles:

- **Preventivos**: Son ejecutados previos a la ejecución de la actividad a la entrada del proceso.
- **Detectivos**: Son los que se realizan durante la ejecución de la actividad.
- **Correctivos**: Son los que se realizan al materializarse el riesgo y requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización.

Así mismo, de acuerdo con la forma como se ejecutan se pueden clasificar en:

- **Control manual**: ejecutados por personas.
- **Control automático**: ejecutados por un sistema o software previamente programado o diseñado.

Análisis y evaluación de los controles

A continuación, se analizan los atributos del control entre atributos de eficiencia y atributos de documentación.

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

Figura 34 Tabla de atributos

Aplicación de los controles en la matriz

Con base en estas características se establece la valoración del control y el desplazamiento del riesgo en el mapa de calor. Los controles preventivos y detectivos generan un desplazamiento en el vector de probabilidad, mientras que los controles correctivos producen un desplazamiento en el vector de impacto.

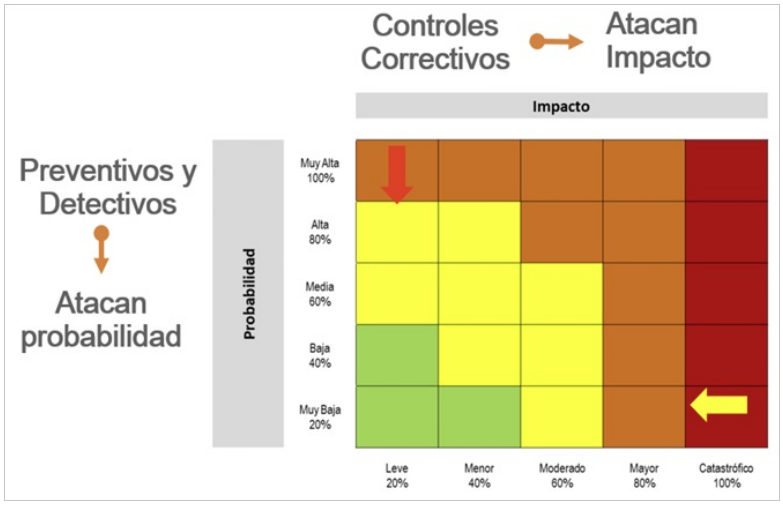


Figura 35 Movimiento matriz de calor

4.6 Riesgo Residual

De acuerdo a la efectividad de los controles se aplicará al riesgo Inherente para mitigar el riesgo de forma acumulativa, una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

A manera de ejemplo a continuación se detalla el cálculo requerido para la aplicación de los controles dependiendo de su tipología.

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

Figura 36 Evaluación riesgo residual

Gráficamente el movimiento en la matriz de calor se muestra de la siguiente manera:

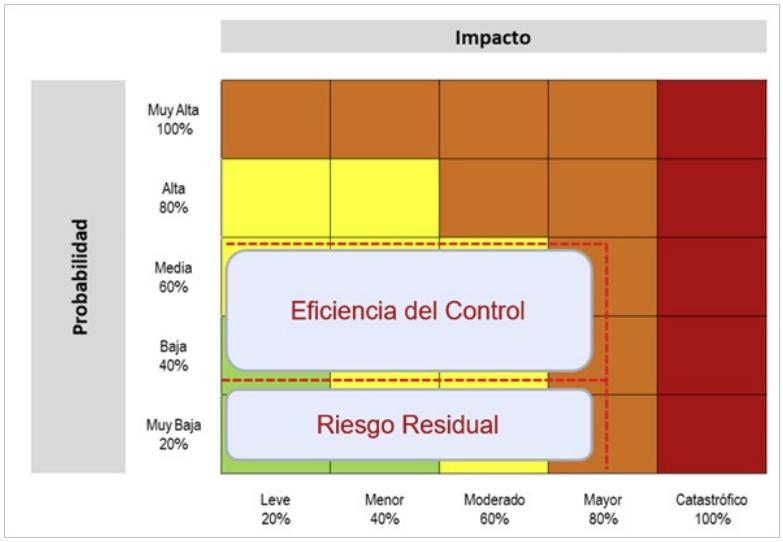


Figura 37 Eficiencia Matriz de Calor

4.7 Tratamiento del riesgo de corrupción

El riesgo de corrupción no se acepta en la Secretaria Distrital de Movilidad (SDM), de acuerdo a la Guía para la gestión integral del riesgo en entidades públicas Versión 7, los riesgos deben tratarse según su nivel, para el caso de corrupción afectan el interés público, tienen impacto legal, disciplinario y penal, y están asociados a la política de integridad.

El riesgo de corrupción no es aceptable para la entidad; por tanto, se establecen controles preventivos, detectivos y correctivos para su mitigación, así como monitoreo permanente a través de las líneas de defensa.

Monitoreo y Revisión

La Secretaría Distrital de Movilidad realizará el monitoreo permanente de los riesgos de corrupción y fraude a través de las líneas de defensa, con el fin de evaluar la efectividad de los controles y detectar oportunamente desviaciones:

- La primera línea de defensa será responsable de la ejecución y reporte de los controles
- La segunda línea realizará la consolidación, análisis y seguimiento
- La tercera línea evaluará de manera independiente la efectividad del sistema.

La revisión de los riesgos se efectuará anualmente o cuando se presenten cambios en el contexto, materialización de eventos o debilidades en los controles, generando las acciones de mejora correspondientes.

En ningún caso los riesgos de corrupción serán objeto de aceptación, por lo cual su monitoreo será permanente y prioritario.

El monitoreo a los riesgos de Corrupción y Fraude se realiza de manera Cuatrimestral con cortes en el mes de abril, agosto y diciembre de acuerdo con lo establecido en la política.

Nota: La Secretaría Distrital de Movilidad (SDM) gestionará los riesgos de Fraude como parte integral del Sistema de Gestión Integral del Riesgo (SIGRIP), aplicando la metodología de identificación, análisis, evaluación, tratamiento y monitoreo establecida en la Guía V7 del DAFP pero como un riesgo independiente.

Los riesgos de Fraude se identificarán bajo la estructura causa–evento–consecuencia, considerando factores internos y externos, así como tipologías de fraude interno, externo, tecnológico y documental. Se establecerán controles preventivos, detectivos y correctivos, especialmente orientados a la segregación de funciones, control de accesos, validaciones automatizadas y auditorías.

El monitoreo se realizará de forma permanente mediante indicadores, reportes y evaluación de eventos, garantizando la mejora continua del sistema. En caso de materialización de un evento de fraude, se activarán los protocolos institucionales de investigación, reporte y mejora del control.

Los riesgos de fraude se abordan como una categoría complementaria a los riesgos de corrupción, diferenciando su naturaleza, pero aplicando la misma estructura metodológica de identificación, análisis, evaluación, tratamiento y monitoreo.

Los riesgos de conflictos de interés se abordan como una categoría complementaria a los riesgos de corrupción, diferenciando su naturaleza, pero aplicando la misma estructura metodológica de identificación, análisis, evaluación, tratamiento y monitoreo.

4.8 Gestión de los Riesgos en el Software MIPG

La Secretaría Distrital de Movilidad (SDM), en el marco de la implementación del Modelo Integrado de Planeación y Gestión (MIPG), cuenta con un software institucional para la administración de riesgos, el cual permite registrar, consolidar y hacer seguimiento a los riesgos identificados en el análisis de contexto.

Para la adecuada gestión en la herramienta, es requisito previo la definición y creación del contexto correspondiente, dentro del cual se agrupan los riesgos identificados. Posteriormente, estos deben ser registrados mediante el diligenciamiento del formulario dispuesto en el sistema, asegurando la consistencia de la información y su alineación con los lineamientos establecidos en la metodología.

4.8.1 Identificación y creación del Riesgo

- **Contexto**: Seleccionar el contexto, esta opción trae relacionado el equipo de trabajo, los criterios de análisis de riesgos y los criterios de evaluación de efectividad de controles.
- **Metodología**: Campo de selección el cual permite definir las reglas de contextualización, identificación de los campos a diligenciar y la evaluación de los controles.
- **Nombre**: Registro del nombre del riesgo
- **Descripción del Riesgo**: Registrar una breve explicación del riesgo
- **Usuario responsable**: Usuario encargado de la identificación y registro del riesgo.

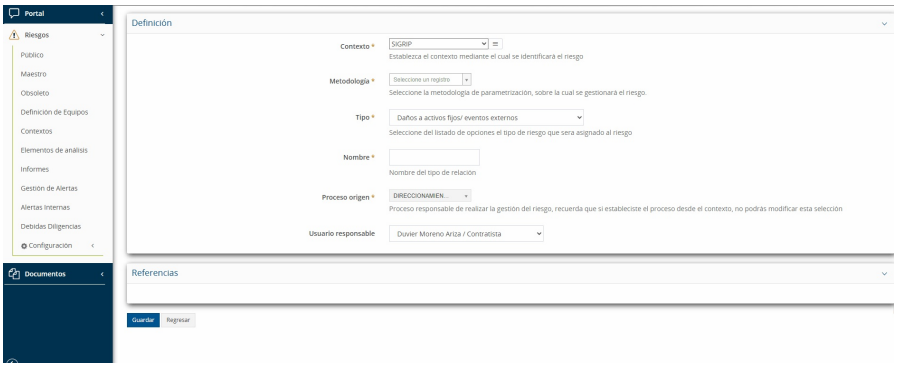


Figura 38 Creación del Riesgo

4.8.2 Etapas de definición del Riesgo

Análisis Risgo Inherente

En el software institucional MIPG, el proceso de gestión del riesgo se desarrolla por etapas. En la etapa de análisis se lleva a cabo la evaluación del riesgo inherente, entendido como la condición del riesgo antes de la implementación o consideración de controles. En esta fase, se realiza la valoración del riesgo mediante la estimación de la **probabilidad** de ocurrencia y el **impacto** de sus consecuencias, con el fin de determinar el nivel de riesgo inherente de la entidad frente a cada evento identificado.

Para los riesgos que hacen parte del contexto de “Riesgos de corrupción”, la determinación de la probabilidad debe efectuarse mediante la selección de criterios independientes, conforme a los lineamientos metodológicos establecidos, garantizando así una valoración objetiva y consistente del riesgo.

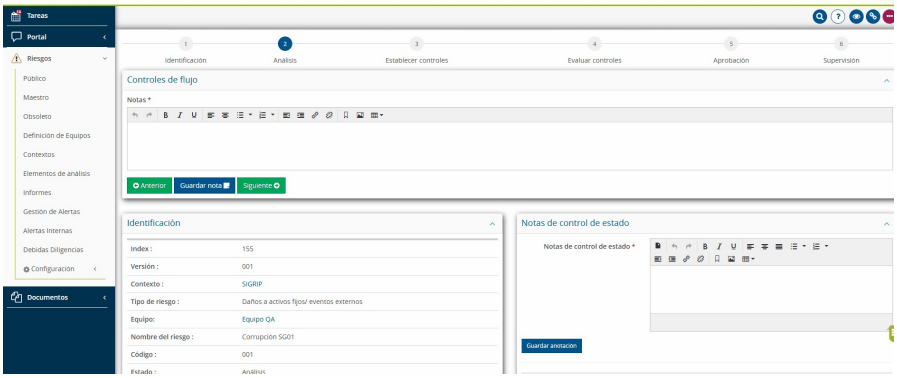


Figura 39 Análisis del Riesgo

4.8.3 Identificación y creación de controles

Desde el Software MIPG los controles se pueden crear de la siguiente manera:

- **Nombre**: Registrar el nombre o abreviatura del control.
- **Descripción**: Ingresar la descripción (Texto) del control, se deben agregar los criterios para validar el cumplimiento del control.
- **Usuario responsable**: Corresponde al usuario responsable del control a cargo de la Oficina Asesora de Planeación Institucional OAPI.
- **Cargo Responsable**: Se debe relacionar el cargo del responsable de ejecutar el control.
- **Periodicidad del Control**: Permite seleccionar el periodo de ejecución del control (Solo una vez, Diario, Semanal, Mensual, Trimestral, Cuatrimestral, Semestral, Anual).

- **Criterio de validación**: Registrar los criterios de validación de efectividad del control, como poder resaltar la evidencia del control.
- **Estado**: Permite seleccionar el estado (activo / Deshabilitado) y definir si es un control obligatorio.

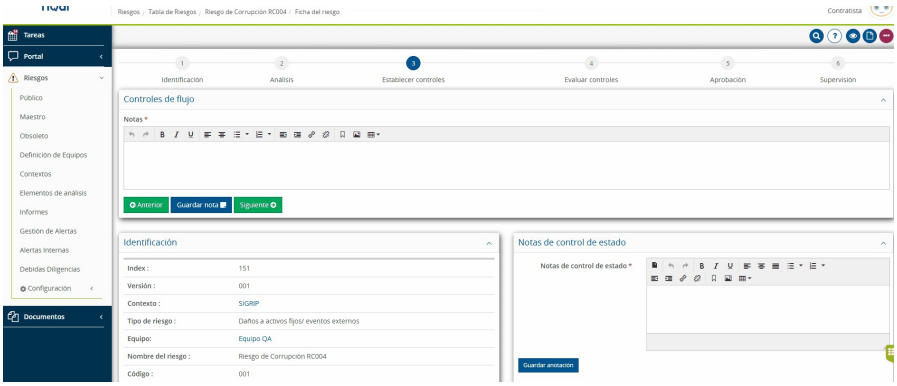


Figura 40 Creación de Controles

Asignación de Tareas

Dentro de la creación de cada control el software permite asignar tareas con el propósito de poder visualizar y contar con las evidencias de los controles.

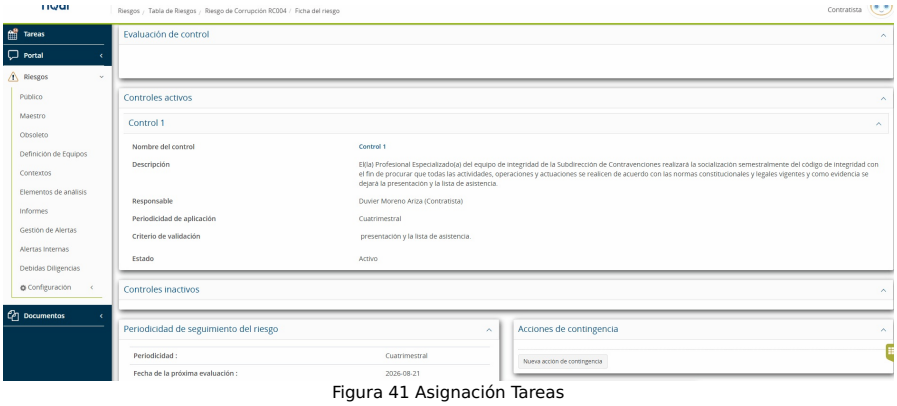


Figura 41 Asignación Tareas

4.8.4 Evaluación de controles

Desde el Software MIPG se puede realizar la evaluación de los controles de la siguiente manera:

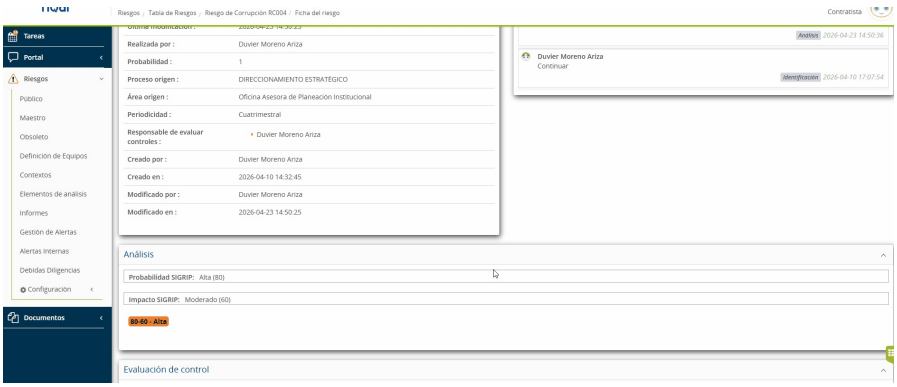


Figura 42 Evaluación de Controles

Para realizar la evaluación es necesario que en cada uno de los criterios se seleccione la respuesta correspondiente, al finalizar la evaluación, el sistema calcula automáticamente si la aplicación de los controles fue efectiva o no e indica el **Riesgo Residual.**

4.8.5 Aprobación

En esta opción se permite evidenciar toda la información del riesgo. Si está conforme con la gestión y proposito se puede agregar una nota y continuar con el riesgo a la etapa de supervisión.

Materialización del Riesgo

El software MIPG cuenta con la opción de poder registrar la materialización del riesgo, en caso de materialización, es decir de que un riesgo se presente en la organización, se convierta en un evento real, este evento puede ser registrado en un formulario donde se puede relacionar el número de veces que se materializó el riesgo, la fecha de materialización y las notas del evento.

5 RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO METODOLOGÍA GUÍA TÉCNICA COLOMBIANA GTC 45:2012

La metodología adoptada por la Secretaría Distrital de Movilidad para la identificación de peligros, evaluación y valoración de riesgos en Seguridad y Salud en el trabajo está basada en la Guía Técnica Colombiana- GTC 45. 2012-06-20, Guía para la Identificación de los Peligros y la Valoración de los Riesgos en Seguridad y Salud Ocupacional, cuenta con los principios fundamentales de la norma NTC- OHSAS 18001 y se basa en el proceso en el proceso de gestión del riesgo desarrollado en la norma BS 8800 (British Standard) y la NTP 330 del Instituto Nacional de Seguridad e Higiene en el Trabajo de España (INSHT) así como en la NTC ISO 31000. Gestión del riesgo. Principios y directrices.

5.1 Los aspectos para tener en cuenta al desarrollar la identificación de los peligros y la evaluación de los riesgos son los siguientes:

- Actividades rutinarias y no rutinarias
- Actividades de todas las personas que tienen acceso al sitio de trabajo (incluyendo a contratistas y visitantes).
- Peligros identificados que se originan fuera del lugar del trabajo con capacidad de afectar adversamente la salud y la seguridad de las personas que están bajo control de la Entidad en el lugar del trabajo.
- Los peligros generados en la vecindad del lugar de trabajo por actividades relacionadas con el trabajo controladas por la Entidad.
- Infraestructura equipo y materiales en lugar de trabajo ya sean suministradas por la Entidad o por otros.
- Cambios realizados o propuestas en la Entidad sus actividades o los materiales.
- Modificaciones al sistema de gestión de seguridad y salud ocupacional, incluidos los cambios temporales y sus impactos sobre las operaciones, procesos y actividades.
- Cualquier obligación legal aplicable relacionada con la valoración del riesgo y la implementación de controles necesarios

- El diseño del área del trabajo, procesos, instalaciones, maquinarias/equipos, procedimientos de operación y Entidad del trabajo incluida su adaptación a las aptitudes humanas.

5.2 Actividades para identificar los peligros y valorar los riesgos

Las siguientes actividades son necesarias para que la SDM, realice la identificación de los peligros y la valoración de los riesgos:

a)La Matriz de identificación de peligros, valoración de riesgos y determinación de controles, se estructura mediante el establecimiento de Grupos de Exposición Similar, los cuales se definen considerando la similitud, la frecuencia y la forma en la que desempeñan las tareas, los materiales y procesos con los cuales los colaboradores (as) trabajan.

b)El formato donde se registra la identificación de peligros, valoración de riesgos y determinación de controles es en el PA02-PR14-F01 Matriz de identificación de peligros, valoración de riesgos y determinación de controles establecido por la Entidad.

c)Clasificar los procesos, las actividades y las tareas: definición de los procesos de trabajo y de cada una de las actividades que lo componen y clasificarlas en donde se incluye instalaciones, planta, personas y procedimientos.

d)Identificar los peligros: incluir todos aquellos relacionados con cada actividad laboral. Considerar quién, cuándo y cómo puede resultar afectado.

e)Identificar los controles existentes: relacionar todos los controles que la SDM ha implementado para reducir el riesgo asociado a cada peligro.

f)Valorar riesgo:

- Evaluar el riesgo: calificar el riesgo asociado a cada peligro, incluyendo los controles existentes que están implementados. Se debe considerar la eficacia de dichos controles, así como la probabilidad y las consecuencias si éstos fallan.
- Definir los criterios para determinar la aceptabilidad del riesgo.
- Definir si el riesgo es aceptable: determinar la aceptabilidad de los riesgos y decidir si los controles de SST existentes o planificados son suficientes para mantener los riesgos bajo control y cumplir los requisitos legales.
- Elaborar el plan de acción para el control de los riesgos, con el fin de mejorar los controles existentes si es necesario, o atender cualquier otro asunto que lo requiera
- Revisar la conveniencia del plan de acción: revalorar los riesgos con base en los controles propuestos y verificar que los riesgos serán aceptables.
- Mantener y actualizar:

a)Realizar seguimiento a los controles nuevos y existentes y asegurar que sean efectivos.

b)Asegurar que los controles implementados son efectivos y que la valoración de los riesgos está actualizada.

c)Se documenta el seguimiento a la implementación de los controles establecidos en el plan de acción que incluye responsables, fecha de programación, ejecución y estado actual, como parte de la trazabilidad de la gestión en SST.

5.3 EXPLICACION DE LA METODOLOGÍA

La metodología establecida permite realizar un proceso sistemático de identificación de peligros, su estimación y valoración de los riesgos propios de la entidad, además de proponer controles generales y específicos al riesgo, de acuerdo con su aceptabilidad.

Los pasos básicos a seguir:

5.3.1 Contexto de la organización.

Implica recolectar la información necesaria para poder adelantar una amplia y completa identificación de los peligros para la seguridad y salud en el trabajo (SST), entre ellas: actividad económica, procesos y servicios con que cuenta, objetivos estratégicos, planeación estratégica, organigrama, información sociodemográfica, tipos de contratación, ubicación geográfica, definición de responsabilidades, políticas de gestión del riesgo.

5.3.2 Identificación de Peligros para la Seguridad y Salud en el Trabajo.

Para la descripción y clasificación de los peligros se debe tener en cuenta la siguiente tabla:

Tabla de Peligros

Descripción	Clasificación						
	Biológico	**Físico**	**Químico**	**Psicosocial**	**Biomecánicos**	**Condiciones de seguridad**	**Fenómenos naturales***
	Virus	Ruido (impacto intermitente y continuo)	Polvos orgánicos inorgánicos	Gestión organizacional (estilo de mando, pago, contratación, participación, inducción y capacitación, bienestar social, evaluación del desempeño, manejo de cambios)	Postura (prologada mantenida, forzada, antigravitacionales)	Mecánico (elementos de máquinas, herramientas, piezas a trabajar, materiales proyectados sólidos o fluidos	Sismo
	Bacterias	Iluminación (luz visible por exceso o deficiencia)	Fibras	Características de la organización del trabajo (comunicación, tecnología, organización del trabajo, demandas cualitativas y cuantitativas de la labor	Esfuerzo	Eléctrico (alta y baja tensión, estática)	Terremoto
	Hongos	Vibración (cuerpo entero, segmentaria)	Líquidos (nieblas y rocíos)	Características del grupo social del trabajo (relaciones, cohesión, calidad de interacciones, trabajo en equipo	Movimiento repetitivo	Locativo (almacenamiento, superficies de trabajo (irregularidades, deslizantes, con diferencia del nivel) condiciones de orden y aseo, caídas de objeto)	Vendaval
	Ricketsias	Temperaturas extremas (calor y frío)	Gases y vapores	Condiciones de la tarea (carga mental, contenido de la tarea, demandas emocionales, sistemas de control, definición de roles, monotonía, etc).	Manipulación manual de cargas	Tecnológico (explosión, fuga, derrame, incendio)	Inundación
	Parásitos	Presión atmosférica (normal y ajustada)	Humos metálicos, no metálicos	Interfase persona tarea (conocimientos, habilidades con relación a la demanda de la tarea, iniciativa, autonomía y reconocimiento, identificación de la persona con la tarea y la organización		Accidentes de tránsito	Derrumbe
	Picaduras	Radiaciones ionizantes (rayos x, gama, beta y alfa)		Jornada de trabajo (pausas, trabajo nocturno, rotación, horas extras, descansos)		Públicos (Robos, atracos, asaltos, atentados, desorden público, etc.)	Precipitaciones, (lluvias, granizadas, heladas)
	Mordeduras	Radiaciones no ionizantes (láser, ultravioleta infraroja)	Material particulado			Trabajo en Alturas	
	Fluidos o excrementos					Espacios Confinados	

* Tener en cuenta únicamente los peligros de fenómenos naturales que afectan la seguridad y bienestar de las personas en el desarrollo de una actividad. En el plan de emergencia de cada empresa se consideraran todos los fenómenos naturales que pudieran afectarla.

Figura 43 Tabla de Peligros

Efectos Posibles

Existen efectos que reflejan consecuencias de cada peligro identificado, es decir que se debe tener en cuenta consecuencias a corto plazo como los de seguridad (accidente de trabajo), y las de largo plazo como las enfermedades laborales.

Igualmente se debe tener en cuenta el nivel de daño que puede generar en las personas.

Tabla No.1. Descripción de Niveles de daño

CATEGORIA DEL DAÑO	DAÑO LEVE	DAÑO MODERADO	DAÑO EXTREMO
Salud	Molestias e irritación ejemplo: dolor de cabeza), enfermedad temporal que produce malestar (ejemplo: diarrea)	Enfermedades que causan Incapacidad temporal. Ejemplo: pérdida parcial de la audición, dermatitis, asma, desórdenes de las Extremidades superiores.	Enfermedades agudas o crónicas, que generan incapacidad permanente parcial, invalidez o muerte.

Seguridad	Lesiones superficiales, heridas de poca profundidad, contusiones, irritaciones del ojo por material particulado.	Laceraciones, heridas profundas, quemaduras de primer grado; conmoción cerebral, esguinces graves, fracturas de huesos cortos.	Lesiones que generen amputaciones, fracturas de huesos largos, trauma cráneo encefálico, quemaduras de segundo y tercer grado, alteraciones severas de mano, de columna vertebral con compromiso de la médula espinal, oculares que comprometan el campo visual, disminuyan la capacidad auditiva

5.4 Identificación de los Controles Existentes

Se debe identificar los controles existentes y relacionar todos los controles que la Entidad ha implementado para reducir el riesgo asociado a cada peligro.

- Fuente: Controles existentes al nivel de la fuente que genera el factor de riesgo.
- Medio: Controles existentes a nivel del medio de transmisión del factor de riesgo.
- Individuo: Controles existentes al nivel de la persona o receptor del factor de riesgo.

Se debe considerar también los controles administrativos que la SDM han implementado para disminuir el riesgo, por ejemplo: inspecciones, ajustes a procedimientos, instructivos, capacitaciones, entre otros.

5.5 Valoración del Riesgo

La valoración del riesgo incluye:

a)la evaluación de los riesgos, teniendo en cuenta la suficiencia de los controles existentes, y

b)la definición de los criterios de aceptabilidad del riesgo,

c)la decisión de si son aceptables o no, con base en los criterios definidos.

5.6 Definición de los criterios de aceptabilidad del riesgo

Para determinar los criterios de aceptabilidad del riesgo, se tiene en cuenta los siguientes aspectos:

- Cumplimiento de los requisitos legales aplicables y otros.
- Su política de SST.
- Objetivos y metas de la SDM.
- Aspectos operacionales, técnicos, financieros, sociales y otros.
- Opiniones de las partes interesadas.

5.7 Evaluación de los riesgos

La evaluación de los riesgos corresponde al proceso de determinar la probabilidad de que ocurran eventos específicos y la magnitud de sus consecuencias, mediante el uso sistemático de la información disponible.

Para evaluar el nivel de riesgo (NR), se debería determinar lo siguiente:

NR = NP x NC

en donde:

NP = Nivel de probabilidad NC = Nivel de consecuenci

A su vez, para determinar el NP se requiere:

NP = ND * NE; donde ND = Nivel de deficiencia y NE = Nivel de exposición

Para determinar el Nivel de Deficiencia (ND) se determina en la siguiente tabla:

Tabla No. 2. Determinación del nivel de deficiencia

NIVEL DE DEFICIENCIA	VALOR DE ND	SIGNIFICADO
Muy Alto (MA	10	Se ha(n) detectado peligro(s) que determina(n) como posible la generación de incidentes o consecuencias muy significativas, o la eficacia del conjunto de medidas preventivas existentes respecto al riesgo es nula o no existe, o ambos.
Alto (A)	6	Se han detectado peligros que pueden dar lugar a consecuencias poco significativas o de menor importancia, o la eficacia del conjunto de medidas preventivas existentes es moderada, o ambos.
Medio (M)	2	Se han detectado peligros que pueden dar lugar a consecuencias poco significativas o de menor importancia, o la eficacia del conjunto de medidas preventivas existentes es moderada, o ambos.
Bajo (B)	No se Asigna Valor	No se ha detectado consecuencia alguna, o la eficacia del conjunto de medidas preventivas existentes es alta, o ambos. El riesgo está controlado.

Tabla No. 3. Determinación del Nivel de Exposición

NIVEL DE EXPOSICION	VALOR DE NE	SIGNIFICADO
Continua (EC)	4	Situación de exposición se presenta sin interrupción o varias veces con tiempo prolongado durante la jornada laboral.
Frecuente (EF)	3	La situación de exposición se presenta varias veces durante la jornada laboral por tiempos cortos.

Ocasional (EO)	2	La situación de exposición se presenta alguna vez durante la jornada laboral y por un periodo de tiempo corto.
Esporádica (EE)	1	La situación de exposición se presenta de manera eventual.

Para determinar el NP se combinan los resultados de las Tablas 2 y 3, en la Tabla 4.

Tabla 4. Determinación Nivel de Probabilidad

NIVEL DE PROBABILIDAD		NIVEL DE EXPOSICIÓN			
		4	3	2	1
Nivel de Deficiencia	10	MA- 40	MA-30	A-20	A-10
	6	MA-24	MA-18	A-12	M-6
	2	M- 8	M-6	B-4	B-2

El resultado de la Tabla 4, se interpreta de acuerdo con el significado que aparece en la Tabla 5.

Tabla 5. Significado de los diferentes niveles de probabilidad

NIVEL DE PROBABILIDAD	VALOR DE NP	SIGNIFICADO
Muy Alto (MA)	Entre 40-20	Situación deficiente con exposición continua, o muy deficiente con exposición frecuente. Normalmente la materialización del riesgo ocurre con frecuencia.
Alto (A)	Entre 20 y 10	Situación deficiente con exposición frecuente u ocasional, o bien situación muy deficiente con exposición ocasional o esporádica. La materialización del riesgo es posible que suceda varias veces en la vida laboral.
Medio (M)	Entre 8 y 6	Situación deficiente con exposición esporádica, o bien situación mejorable con exposición continuada o frecuente. Es posible que suceda el daño alguna vez.
Bajo (B)	Entre 4 y 2	Situación mejorable con exposición ocasional o esporádica, o situación sin anomalía destacable con cualquier nivel de exposición. No es esperable que se materialice el riesgo, aunque puede ser concebible

A continuación, se determina el nivel de consecuencias según los parámetros de la Tabla 6.

Tabla 6. Determinación del nivel de consecuencias

NIVEL DE CONSECUENCIA	NC	SIGNIFICADO
Mortal o catastrófico (M)	100	Muerte (s)
Muy Grave (MG)	60	Lesiones o enfermedades graves irreparables (Incapacidad permanente parcial o invalidez).
Grave (G)	25	Lesiones o enfermedades con incapacidad laboral temporal (ILT).
Leve (L)	10	Lesiones o enfermedades que no requieren incapacidad.

NOTA: Para evaluar el nivel de consecuencias, se debe tener en cuenta la consecuencia directa más grave que se pueda presentar en la actividad valorada.

Los resultados de las Tablas 5 y 6 se combinan en la Tabla 7 para obtener el nivel de riesgo, el cual se interpreta de acuerdo con los criterios de la Tabla 8.

Tabla 7. Determinación del nivel de riesgo

NIVEL DEL RIESGO NR= NP X NC		**NIVEL DE PROBABILIDAD (NP)**			
		40-24	**20-10**	**8-6**	**4-2**
Nivel de Consecuencias(NC)	100	**I 4000- 2400**	**I 2000-1200**	**I 800-600**	**II 400-200**
	60	**I 2400-1400**	**I 1200-600**	**II 480-360**	**II200 III 120**
	25	**I 1000-600**	**II 500 – 250**	**II 200-150**	**III 100-50**
	10	**II 400-240**	**II 200 III 100**	**III 80-60**	**III 40 IV 20**

Tabla 8. Significado del nivel de riesgo

NIVEL DEL RIESGO	VALOR DEL NR	SIGNIFICADO
I	4 000- 600	Situación crítica. Suspender actividades hasta que el riesgo esté bajo control. Intervención urgente.
II	500-150	Corregir y adoptar medidas de control de inmediato. Sin embargo, suspenda actividades si el nivel de riesgo está por encima o igual de 360.
III	120-40	Mejorar si es posible. Sería conveniente justificar la intervención y su rentabilidad
IV	20	Mantener las medidas de control existentes, pero se deberían considerar soluciones o mejoras y se deben hacer comprobaciones periódicas para asegurar que el riesgo aún es aceptable.

Decidir si el riesgo es aceptable o no

Una vez determinado el nivel de riesgo, la Entidad debe decidir cuáles riesgos son aceptables y cuáles no. En una evaluación completamente cuantitativa es posible evaluar el riesgo antes de decidir el nivel que se considera aceptable o no aceptable. Sin embargo, con métodos semi cuantitativos tales como el de la matriz de riesgos, la Entidad deberé establecer cuáles categorías son aceptables y cuáles no.

Para hacer esto, la Entidad debe primero establecer los criterios de aceptabilidad, con el fin de proporcionar una base que brinde consistencia en todas sus valoraciones de riesgos. Esto debe incluir la consulta a las partes interesadas y debe tener en cuenta la legislación vigente.

Tabla 9. Aceptabilidad del riesgo

NIVEL DEL RIESGO	**SIGNIFICADO**
I	No Aceptable
II	No Aceptable o Aceptable con control específico
III	Aceptable
IV	Aceptable

Al aceptar un riesgo específico, se debe tener en cuenta el número de expuestos y las exposiciones a otros peligros, que puede aumentar o disminuir el nivel de riesgo en una situación particular.

La exposición al riesgo individual de los miembros de los grupos especiales también se debe considerar, por ejemplo, los grupos vulnerables, tales como nuevos o inexpertos.

Elaborar el plan de acción para el control de los riesgos

Los niveles de riesgo, como se muestra en la Tabla 8, forman la base para decidir si se requiere mejorar los controles y el plazo para la acción. Igualmente muestra el tipo de control y la urgencia que se debería proporcionar al control del riesgo.

El resultado de una valoración de los riesgos debería incluir un inventario de acciones, en orden de prioridad, para crear, mantener o mejorar los controles.

5.8 Criterios para establecer controles

Si existe una identificación de los peligros y valoración de los riegos en forma detallada es mucho más fácil para la Entidad determinar qué criterios necesita para priorizar sus controles, sin embargo, en la práctica este proceso debe tener como mínimo los siguientes tres (3) criterios:

Número de expuestos: Número de personal involucrado en ese Grupo a área de trabajo tanto de planta como contratistas.

Peor consecuencia: Se determinará el mayor efecto posible en la salud del trabajador. Ejemplo: Exposición a Peligro Químico su peor consecuencia - Enfermedades pulmonares, Irritación ocular, Irritación vías respiratorias, Irritación de la piel, Lesiones oculares graves, Intoxicación sistémica, Efectos asfixiantes y/o Muerte. (Estas ya se encuentran por cada Peligro en la hoja Listas)

Existe requisito legal específico asociado: La Entidad establece si existe o no un requisito legal especifico a la tarea que se está evaluando para tener parámetros en priorización en la implementación de medidas de intervención. Se referencian los generales.

5.9 Medidas de intervención

Una vez completada la valoración de los riesgos, la Entidad deberá estar en capacidad de determinar si los controles existentes son suficientes o necesitan mejorarse. Para esto debe proponer los controles necesarios y pertinentes, bien sean de eliminación, sustitución, controles de ingeniería, controles administrativos o equipos y elementos de protección.

Eliminación: "Modificar un diseño para eliminar el peligro, por ejemplo, introducir dispositivos mecánicos de alzamiento para eliminar el peligro de manipulación manual (Definición GTC - 45). Medida que se toma para suprimir (hacer desaparecer) el peligro/riesgo. (Definición Decreto 1072/2015)"

Sustitución: "Reemplazar por un material menos peligroso o reducir la energía del sistema (por ejemplo, reducir la fuerza, el amperaje, la presión, la temperatura, etc.) (Definición GTC - 45). Medida que se toma a fin de remplazar un peligro por otro que no genere riesgo o que genere menos riesgo. (Definición Decreto 1072/2015)"

Control de ingeniería: "Instalar sistemas de ventilación, protección para las máquinas, enclavamiento, cerramientos acústicos, etc. (Definición GTC - 45). Medidas técnicas para el control del peligro/riesgo en su origen (fuente) o en el medio, tales como el confinamiento (encerramiento) de un peligro o un proceso de trabajo, aislamiento de un proceso peligroso o del trabajador y la ventilación (general y localizada), entre otros. (Definición Decreto 1072/2015) "

Controles administrativos, señalización, advertencia: Instalación de alarmas, procedimientos de seguridad, inspecciones de los equipos, controles de acceso, capacitación del personal. (Definición GTC - 45). Medidas que tienen como fin reducir el tiempo de exposición al peligro, tales como la rotación de personal, cambios en la duración o tipo de la jornada de trabajo. Incluyen también la señalización, advertencia, demarcación de zonas de riesgo, implementación de sistemas de alarma, diseño e implementación de procedimientos y trabajos seguros, controles de acceso a áreas de riesgo, permisos de trabajo, entre otros. (Definición Decreto

1072/2015) "

Equipos y elementos de protección personal: "Dar recomendaciones referentes al control de elementos de protección persona o equipos que sean necesarios ej: gafas de seguridad, protección auditiva, mascaras faciales, sistemas de detención decaídas, respiradores y guantes. Etc. (Definición GTC - 45). Medidas basadas en el uso de dispositivos, accesorios y vestimentas por parte de los trabajadores, con el fin de protegerlos contra posibles daños a su salud o su integridad física derivados de la exposición a los peligros en el lugar de trabajo. El empleador deberá suministrar elementos y equipos de protección personal (EPP) que cumplan con las disposiciones legales vigentes. Los EPP deben usarse de manera complementaria a las anteriores medidas de control y nunca de manera aislada, y de acuerdo con la identificación de peligros y evaluación y valoración de los riesgos. (Definición Decreto 1072/2015) "

Al aplicar un control determinado se debe considerar los costos relativos, los beneficios de la reducción de riesgos, y la confiabilidad de las opciones disponibles.

Plan de acción

El plan de acción frente a los controles establecidos se incluirá en la matriz de registro y seguimiento a la ejecución de las oportunidades de mejora del SG-SST.

5.10 Mantenimiento y actualización

La SDM debe identificar los peligros y evaluar los riesgos periódicamente.

La determinación de la frecuencia se puede dar por alguno o varios de los siguientes aspectos:

- La necesidad de determinar si los controles para el riesgo existentes son eficaces y suficientes.
- La necesidad de responder a nuevos peligros.
- La necesidad de responder a los cambios que la propia Entidad ha llevado a cabo.
- La necesidad de responder a retroalimentación de las actividades de seguimiento, investigación de incidentes, situaciones de emergencia o los resultados de las pruebas de los procedimientos de emergencia.
- Cambios en la legislación.
- Factores externos, por ejemplo, problemas de SST que se presenten.
- Avances en las tecnologías de control.
- La diversidad cambiante en la fuerza de trabajo, incluidos los contratistas.

No es necesario llevar a cabo nuevas valoraciones de los riesgos cuando una revisión puede demostrar que los controles existentes o los planificados siguen siendo eficaces.

5.11 Seguimiento de las medidas de control para garantizar que continúen siendo adecuadas

Luego de implementadas las medidas para el tratamiento para los riesgos, es necesario hacer seguimiento a su implementación, efectividad y permanencia en el tiempo. Este seguimiento debe programarse y realizarse a través de inspecciones o auditorias del Sistema de gestión.

5.12 Revisión de la valoración de riesgos

En forma periódica y cuando las condiciones cambien se debe realizar una revisión de la valoración de riesgos a fin de garantizar que:

- Se incluyan los peligros nuevos provenientes de cambios o modificaciones.
- Se modifique la evaluación del riesgo luego de implementadas las medidas para el tratamiento del riesgo.

Algunos puntos para revisar son

- Cambio en la naturaleza del trabajo o actividad.
- Fallas o debilidades en los controles reveladas por las inspecciones de seguridad, las auditorías, las investigaciones de accidentes e incidentes (análisis de causalidad de los mismos).
- Desarrollo de análisis de seguridad más profundos a riesgos específicos.
- Nueva legislación.
- Cambios en los procesos o servicios.
- Cambio o mejora de equipos.

Comunicación de los Riesgos

La matriz de identificación de peligros, valoración de riesgos y determinación de controles y su información se debe considerar como documento controlado, debe estar disponible para la consulta y análisis tanto del personal planta como de los contratistas y debe publicarse en la intranet.

6 METODOLOGÍA PARA LA IDENTIFICACIÓN, EVALUACIÓN Y TRATAMIENTO DE RIESGOS DE SOBORNO

Introducción

La presente metodología se encuentra articulada con la Guía de administración del riesgo y el diseño de controles en entidades públicas del DAFP versión 7, esto con el fin de tener un mayor alcance y robustez en la gestión de riesgos de soborno y de cara al mantenimiento del Sistema de Gestión Antisoborno que tiene implementado la Entidad y a las mejores prácticas reflejadas en la NTC ISO 37001.

Objetivo

Establecer la metodología para la identificación, evaluación y tratamiento de los riesgos de soborno que se puedan presentar en las diversas actividades en las que hay interacción con externos.

6.1 Responsabilidades

Tabla 10. Responsabilidades - lineas de defensa riesgos de soborno

LINEA DE DEFENSA	RESPONSABLE	RESPONSABILIDADES
Línea Estratégica	**Comité Institucional de Gestión y Desempeño – CIGD**	• Revisar el contexto estratégico, plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el fin de analizar los posibles eventos de riesgos que se puedan materializar en el ejercicio de las funciones de la Entidad. • Establecer y aprobar la Política de Administración del Riesgo para la Secretaría Distrital de Movilidad - SDM. • Analizar el informe de seguimiento a la gestión del riesgo, con el fin de proponer acciones de mejora y gestionar la toma de decisiones.
		• Apoyar la implementación de la política para la administración del riesgo. • Revisar e identificar los posibles hechos de soborno determinados a sus áreas, sedes, procesos y actividades.

Primera Línea	**Miembros del Equipo Técnico de Calidad (Enlaces SGAS) y/o Líderes de proceso**	• Identificar y documentar los controles para evitar la materialización de los riesgos. • Socializar con sus áreas la matriz de riesgos de soborno garantizando la participación de los jefes de las mismas. • Realizar el monitoreo periódico a la matriz de riesgos de soborno para garantizar la aplicación de los controles. • Realizar el reporte periódico y oportuno de las evidencias de cumplimiento de los controles. • Informar al Oficial de Cumplimiento cada vez que se requiera ajustar la matriz de riesgos de soborno de su proceso. • Socializar los informes de seguimiento de la matriz de riesgos de soborno con los dueños de los procesos. • Verificar que las evidencias reportadas estén acordes con las definidas en los controles para la mitigación del riesgo
	Oficial de cumplimiento	• Acompañar metodológicamente a los procesos en la construcción o actualización del mapa de riesgo. • Realizar la evaluación de probabilidad e impacto de cada uno de los posibles hechos de soborno identificados.
Segunda Línea	Oficial de Cumplimiento	• Definir la metodología para la administración del riesgo, acorde a la normatividad y lineamientos de la norma antisoborno. • Adelantar el monitoreo de los mapas de riesgos, evaluando la eficacia de los controles y los cambios de valoración del riesgo residual que se presenten en el ejercicio de la gestión del riesgo. • Consolidar y publicar el mapa, acorde a los lineamientos normativos • Revisar periódicamente la matriz de riesgos de soborno. • Aprobar la matriz de riesgos de soborno. • Socializar en el Comité Institucional de Gestión y Desempeño la matriz de riesgos de soborno. • Definir los controles antisoborno a aplicar a los riesgos con calificación de moderado, alto o extremo que se determinen en la matriz de riesgos de soborno. • Aprobar el plan de tratamiento de riesgos. • Generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas. • Verificar que las evidencias reportadas estén acordes con las definidas en los controles para la mitigación del riesgo.
	Equipo Técnico Antisoborno	• Revisar la gestión realizada sobre los riesgos con calificación de moderado, alto o extremo. • Tomar decisiones frente a los controles que no sean efectivos. • Realizar seguimiento a los planes de tratamiento de los riesgos de soborno.
Tercera Línea	**Oficina de Control Interno - OCI**	• Generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas, a partir de auditorías, seguimientos y/o monitoreos, según actividades programadas en el PAAI aprobado (según selectivo). • Verificar la aplicación metodológica de la guía para la gestión del riesgo en la SDM y la aplicación de la política. • Evaluar la efectividad de los controles y planes de acción propuestos, según selectivo y programación del PAAI aprobado para la vigencia. • Publicar los seguimientos realizados a los mapas de riesgo.

6.2 Metodología riesgos de soborno

La metodología para los riesgos de sobrono se realiza bajo los lineamientos definidos por el Departamento Administrativo de la Función Pública - Guía para la gestión Integral del riesgo en entidades públicas versión 7 de agosto de 2025.

6.2.1 Identificación del riesgo

La identificación es la etapa donde se analizan los riesgos que están bajo el control de la organización, para la cual se debe tener en cuenta el contexto estratégico en el que opera la entidad, de igual manera el análisis de los factores internos y externos que afecten el cumplimiento de los objetivos institucionales.

a. Análisis de objetivos estratégicos y de los procesos:

Análisis de objetivos estratégicos	Análisis de objetivos del proceso
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso, así mismo, los objetivos asociados al sistema de gestión antisoborno.	Los objetivos de los procesos deben estar alineados con los objetivos estratégicos, así como con la misión, visión y objetivos del SGAS.

Cadena de valor

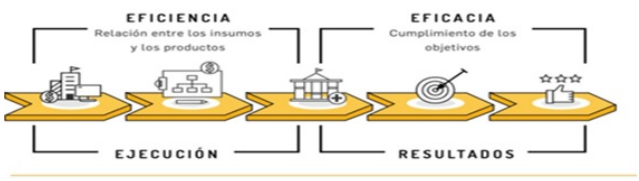


Figura 44 Cadena de valor

Por medio de la cadena de valor se pueden identificar las actividades que están dentro del flujo del proceso y a partir de éstas identificar la posibilidad de presentarse la materialización de un riesgo en el cumplimento de los objetivos del proceso, del sistema de gestión antisoborno o de la entidad.

b. Área de impacto
El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional, para algunos riesgos puede presentarse que la afectación sea de tipo económica y reputacional a la vez.
c. Áreas de factores de riesgo
Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

FACTOR	DESCRIPCION	DESCRIPTOR
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Soborno

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

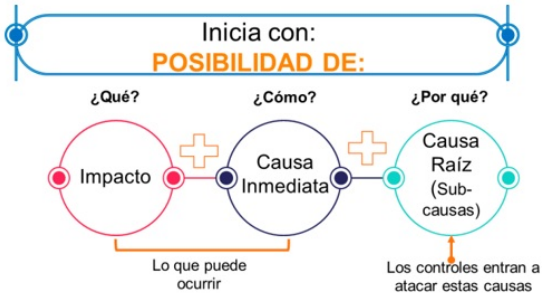


Figura 45 Estructura para la redacción del riesgo

Es importante tener presente que para la redacción de los riesgos de soborno se debe: revisar la documentación de cada uno de los procesos de la Entidad para identificar posibles hechos de soborno y los controles, documentar quién es la persona responsable de ejecutar los controles, la periodicidad con que se aplicará, el soporte que quedará como evidencia de la ejecución del mismo y validar que los posibles hechos de soborno identificados correspondan con las actividades propias del proceso y del área, así mismo, los controles y responsables de los mismos.

Ejemplo:

Redacción inicia con:	**IMPACTO** **¿Qué?**	**CAUSA INMEDIATA** **¿Cómo?**	**CAUSA RAIZ** **¿Por qué?**
Posibilidad de	afectación reputacional	por aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero,	a causa de la manipulación indebida de sistema de información de asignación de citas.

Redacción final del riesgo: Posibilidad de afectación reputacional por aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.

Premisas para una adecuada redacción del riesgo:

- No describir como riesgos fallas ni desviaciones del control.
- No describir riesgos como la negación de un control.
- No existen riesgos transversales, lo que pueden existir son causas transversales.

6.2.2 Valoración del riesgo

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

a. **Tabla de probabilidad**: Teniendo en cuenta el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, la cual se describe en la siguiente tabla, que establece los criterios para definir el nivel de probabilidad.

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Figura 46 Criterios para definir el nivel de probabilidad

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

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

Figura 47 Criterios para definir el nivel de impacto

La valoración de riesgos se realizará en conjunto entre el líder y/o el enlace de calidad del proceso y el Oficial de Cumplimiento y/o su delegado, con el fin de mantener la imparcialidad frente a la valoración que se viene manejando desde el Sistema de Gestión Antisoborno.

6.2.3 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 residual (RIESGO INHERENTE).

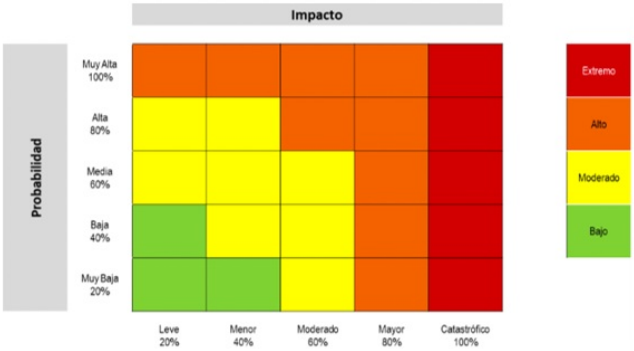


Figura 48 Matriz de calor (niveles de severidad del riesgo)

6.2.4 Valoración de controles

Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.
- Los responsables de implementar y monitorear los controles son las/los líderes de proceso con el apoyo de su equipo de trabajo.

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

- **Responsable de ejecutar el control:** Identifica el cargo de la/el servidor (a) 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.

Figura 49 Estructura para la redacción de controles

Ejemplo:

RESPONSABLE	ACCION	COMPLEMENTO
El profesional de la Dirección de Contratación	verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos al tipo de contratación,	a través de la lista de chequeo de requisitos, se revisa frente a la información suministrada por el proveedor, si este cumple se registra en el sistema de información de contratación.

Redacción final del control: El profesional de la Dirección de Contratación verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos al tipo de contratación, a través de la lista de chequeo de requisitos, se revisa frente a la información suministrada por el proveedor, si este cumple se registra en el sistema de información de contratación.

6.2.5 Tipología de controles

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

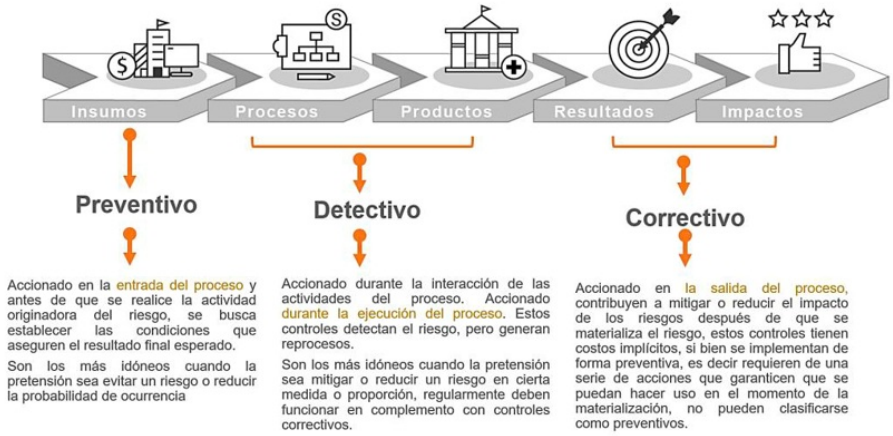


Figura 50 Cadena de valor del proceso y las tipologías de controles

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

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

- **Control manual:** Son ejecutados por personas.
- **Control automático:** Ejecutados por un sistema o software previamente programado o diseñado.

6.2.6 Valoración de controles

A continuación, se analizan los atributos del control:

Tabla 11. Valoración de controles de soborno

CARACTERISTICAS DE EFICIENCIA		PESO
TIPO	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
IMPLEMENTACION	Automático	25%
	Manual	15%

CARACTERISTICAS DE EFICIENCIA		DESCRIPCIÓN
DOCUMENTACION	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros esquemas	Políticas de operación, manuales o guías específicas.
FRECUENCIA	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral)	
EVIDENCIA (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
EJECUCIÓN (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Los atributos de formalización solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que del valor de los atributos se genera el movimiento del mapa de calor, se debe tener en cuenta los tipos de movimientos dependiendo del tipo de control implementado.

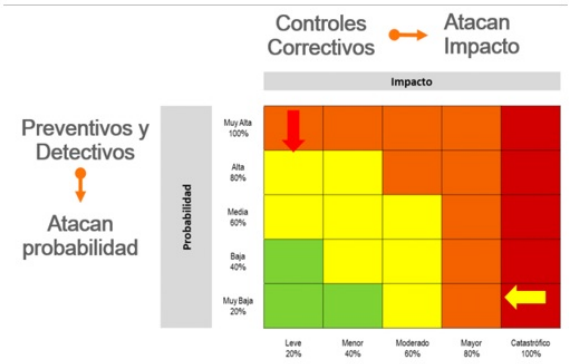


Figura 51 Movimiento en la matriz de calor acorde con el tipo de control

6.2.7 Valoración de riesgo residual

Con esta información se procede a realizar el cálculo del nivel de riesgo residual de la siguiente manera.

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

Figura 52 Aplicación de controles para establecer el riesgo residual

6.3 Lineamientos y/o políticas de operación

- La matriz de riesgos de soborno será revisada una vez al año con el fin de identificar nuevos riesgos y/o actualizar los controles para cada uno de ellos; a menos que por el estado del proceso o por su nivel de importancia sea necesario hacerlo con mayor frecuencia.
- Se deberán contemplar todos los procesos de la Entidad para la identificación de riesgos de soborno.
- Esta actualización es responsabilidad del Oficial de Cumplimiento quien, con el apoyo del Equipo Técnico de Calidad, revisará y actualizará el mapa de riesgos de soborno.
- Es necesario que las personas y partes involucradas tanto internas como externas, estén informadas sobre los riesgos a los cuales se encuentran expuestos y que se establezcan los mecanismos de consulta y comunicación con el fin de mantener informados de este proceso.
- El Equipo Técnico de Calidad deberá garantizar que los controles se estén ejecutando conforme se documenten en la matriz, en el caso de algún cambio en estos controles deberá solicitar la actualización al Oficial de Cumplimiento.
- El Oficial de Cumplimiento y/o Equipo Antisoborno realizarán el monitoreo al mapa de riesgos de soborno, con corte al 31 de enero y 31 de julio de cada vigencia, y lo comunicarán y publicarán en la página web de la SDM, en el link de transparencia y acceso a la información pública, para conocimiento de las partes interesadas.
- Producto del seguimiento semestral al mapa de riesgos de soborno el Oficial de Cumplimiento emitirá informe de resultados de la evaluación de los controles y del plan de tratamiento.
- El Oficial de Cumplimiento socializará ante la Alta Dirección los resultados del seguimiento a la matriz de riesgos de soborno mediante memorando.

6.4 Materialización de riesgos de soborno

En el caso de la materialización de un riesgo de soborno se deberá aplicar lo establecido en la política de riesgos de SIGRIP.

7 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BAJO LA METODOLOGÍA DEL DEPARTAMENTO DE FUNCIÓN PÚBLICA GUÍA PARA LA GESTIÓN INTEGRAL DEL RIESGO VERSIÓN 7.0 Y LINEAMIENTOS DEL MODELO NACIONAL DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS DE MINTIC

7.1 Metodología de Gestión de Riesgos de Seguridad de la Información

La metodología de Gestión de Riesgos de Seguridad de la información de la Secretaría Distrital de Movilidad se fundamenta en la integración de la metodología del Departamento Administrativo de la Función Pública y los lineamientos del modelo nacional de gestión de riesgos en el marco del modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones, como habilitador de la Política de Gobierno Digital. Esta metodología adopta un enfoque sistemático para la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar los activos de información de la entidad, considerando los criterios de seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

7.2 Identificación de activos de la información

Para la identificación de los riesgos de seguridad de la Información, los procesos de la Secretaría Distrital de Movilidad deben realizar de manera previa la identificación de los Activos de Información, de conformidad con lo establecido en el PA04-IN03 Instructivo para la identificación, clasificación y valoración de activos de información. Esta actividad constituye el insumo base para la gestión del riesgo en seguridad de la información, puesto que permite reconocer los activos que soportan los procesos de la entidad y sobre los cuales pueden materializarse eventos que afecten los criterios de seguridad de la información.

Una vez los activos de información han sido identificados, clasificados, valorados y determinada su criticidad; aquellos cuya criticidad se encuentre categorizada en nivel "Crítico" serán considerados como insumo para la identificación de riesgos, con el propósito de gestionarlos mediante la aplicación de la presente metodología de gestión de riesgos de seguridad de la información.

7.3 Identificación del riesgo de seguridad de la información

El objetivo de esta fase es determinar el nivel inherente del riesgo al que están expuestos los activos de información críticos, mediante la identificación de sus vulnerabilidades, amenazas y consecuencias, así como la estimación de las probabilidades de ocurrencia y los impactos asociados. Para realizar esta identificación, es fundamental contar con la participación del propietario del activo de información y/o su equipo de trabajo, quienes conocen el contexto y la operación y el uso del

activo dentro del proceso.

Una vez identificados y seleccionados los activos de información objeto de la gestión de riesgos, se debe determinar el atributo de seguridad predominante que podría verse comprometido ante la materialización del riesgo. de acuerdo con los siguientes criterios:

- **Pérdida de la confidencialidad**: Riesgo de divulgación, acceso o uso no autorizado de la información.
- **Pérdida de la integridad:** Riesgo de alteración, modificación o corrupción de los datos, lo que impacta la exactitud y confiabilidad.
- **Pérdida de la disponibilidad:** Riesgo de Interrupción o pérdida de acceso oportuno a la información y servicios, afectando la continuidad operativa del proceso.

Para cada riesgo identificado, se debe asociar el activo o grupo de activos críticos del proceso correspondiente y analizar las posibles amenazas, vulnerabilidades y consecuencias que podrían dar lugar a la materialización del riesgo.

a) Identificación de Amenazas y vulnerabilidades

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

Amenaza: Causa potencial de un incidente no deseado, que puede explotar una vulnerabilidad y generar un impacto negativo sobre un activo de información, Las amenazas pueden ser de origen interno o externo, intencionales o accidentales, y pueden estar relacionadas con factores humanos, tecnológicos, físicos o ambientales.

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

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

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

Para la identificación de las amenazas y vulnerabilidades a las que está expuesto cada activo de información, se puede utilizar como referencia el documento “PE01-G01-F03 Formato matriz de consulta de amenazas, vulnerabilidades y controles para la gestión de riesgos de seguridad de la información”, el cual incluye la tabla de amenazas comunes, la tabla de vulnerabilidades comunes y la tabla de controles, diseñadas como herramientas de apoyo para las áreas en el análisis y gestión de riesgos de seguridad de la información.

b) Identificación de Consecuencias

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

c) Descripción del riesgo

La descripción del riesgo debe elaborarse de manera estructurada, evidenciando la relación entre sus elementos: vulnerabilidad, amenaza y consecuencia. Para tal efecto, se adopta la siguiente estructura de redacción.

La pérdida de la confidencialidad, integridad o disponibilidad de la información del ACTIVO DE INFORMACIÓN puede ser ocasionada por LA VULNERABILIDAD, la cual puede ser explotada por una(s) AMENAZA(s) generando posibles CONSECUENCIAS para la entidad.

A continuación, se presenta un ejemplo que muestra la forma adecuada de describir un riesgo de seguridad de la información.

Tabla 12. Ejemplo descripción del Riesgo

Proceso	Activo de Información	Tipo de Riesgo	Vulnerabilidad	Amenaza	Consecuencia	Descripción del Riesgo
Gestión del Talento Humano	Base de datos de nómina	Pérdida de la Confidencialidad	Ausencia de controles adecuados de acceso lógico	Acceso no autorizado	Divulgación no autorizada de información personal y financiera, posibles sanciones legales y afectación reputacional	La pérdida de la confidencialidad de la información de la base de datos de nómina puede ser ocasionada por la ausencia de controles adecuados de acceso lógico, la cual puede ser explotada por accesos no autorizados, generando sanciones legales y afectación reputacional.

Fuente: Adaptada de la Guía para la Gestión Integral del riesgo en entidades públicas- Versión 7-DAFP y ajustado por la OTIC

7.4 Análisis del Riesgo Inherente

En esta etapa se busca establecer la probabilidad de ocurrencia e impacto asociado a la materialización de los riesgos inherentes, con el fin de estimar el nivel o zona de riesgo inherente.

7.4.1 Determinación de la probabilidad Inherente

La probabilidad inherente corresponde a la posibilidad de ocurrencia de un riesgo de seguridad de la información, asociada al nivel de exposición del riesgo del proceso o actividad que se está analizando y sin considerar la existencia de controles. En este sentido, la probabilidad se determina con base en la frecuencia de uso del activo de información dentro del periodo de un año.

A mayor frecuencia de uso del activo de información, mayor será su nivel de exposición al riesgo y por ende mayor probabilidad de ocurrencia.

La determinación de la probabilidad inherente por frecuencia de la actividad se realizará de acuerdo con la siguiente tabla:

	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%

Figura 53 Probabilidad

El líder del proceso, en su calidad de propietario del activo de información y conocedor de las actividades a su cargo, define la frecuencia con que se utiliza cada activo de información, lo cual permite asignar el nivel de probabilidad inherente correspondiente conforme a la escala establecida.

7.4.2 Determinación del Impacto Inherente

El impacto inherente se define como la magnitud del daño o consecuencia que tendría la materialización de un riesgo sobre un activo de información, considerando su criticidad y sin aplicar controles.

La determinación del impacto inherente contempla las posibles consecuencias económicas o reputacionales, derivadas de la materialización del riesgo. Para su valoración, el propietario del activo de información asigna el nivel de impacto correspondiente utilizando la siguiente tabla:

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

Figura 54 Impacto

7.4.3 Evaluación del nivel del riesgo inherente

El nivel de riesgo inherente se determina mediante la combinación de los resultados obtenidos en la evaluación de probabilidad y el impacto. Esta combinación permite ubicar el riesgo dentro de una de las zonas definidas en el mapa de calor, facilitando su interpretación y priorización.

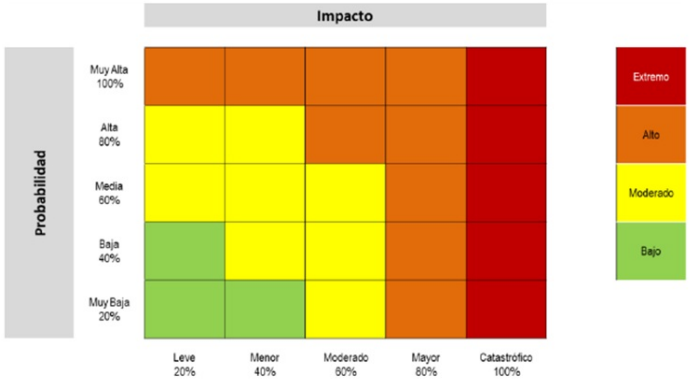


Figura 55 Nivel del Riesgo Inherente

7.4.4 Identificacicación de Controles

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

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

La entidad adopta como referencia mínima los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2022, aunque se pueden definir controles adicionales de acuerdo con las necesidades de la entidad. Como apoyo para la identificación y selección de dichos controles, estos se encuentran relacionados y consolidados en el documento “PE01-G01-F03 Formato matriz de consulta de amenazas, vulnerabilidades y controles para la gestión de riesgos de seguridad de la información”.

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

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

Tabla N° 13. Ejemplo de identificación de Controles

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

7.4.5 Valoración de Controles

A continuación se presentan los atributos utilizados para el diseño, implementación y valoración de controles en el marco de la gestión de riesgos de seguridad de la información. Los atributos sin peso son atributos informativos que no tienen incidencia en la eficiencia del control.

Tabla N° 14. Atributos de Controles

Características			**Descripción**	**Peso**
	Tipo	Preventivo	Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.	25%
		Detectivo	Aquellos que se activan durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos	15%

Atributos de Eficiencia		Correctivo	Aquellos que permiten el restablecimiento de la actividad, una vez se ha detectado un evento no deseable; así como la modificación de las acciones que propiciaron su ocurrencia.	10%
	Implementación	Automático	Aquellos que son ejecutados a través de un sistema de información o aplicativo.	25%
		Manual	Aquellos que son operados o ejecutados por una persona.	15%
Atributos Informativos	Documentación	Documentado	Controles que están documentados en el proceso ya sea en manuales, procedimientos o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica aquellos controles que se ejecutan en el proceso pero que no se encuentran documentados, en ningún documento del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	-
	Evidencia	Con Registro	El control deja un registro, se evidencia la ejecución del control.	-
		Sin Registro	El control no deja registro de la ejecución del control.	-

Con base en estos criterios se establece la valoración del control y, consecuencia, el desplazamiento del riesgo en el mapa de calor. En este contexto, los controles preventivos y detectivos generan un desplazamiento en el vector de probabilidad, mientras que los controles correctivos producen un desplazamiento en el vector de impacto.

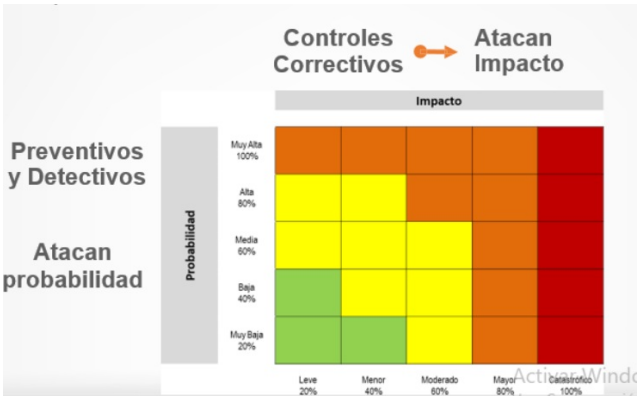


Figura 56 Movimiento en la matriz de calor acorde con el tipo de control

Fuente:Guía para la Gestión Integral del riesgo en entidades públicas- Versión 7-DAFP

7.5 Identificación del riesgo residual

Una vez aplicados los controles definidos para la mitigación de un riesgo, se procede al cálculo del riesgo residual, entendido como el nivel de riesgo que persiste después de la implementación de las medidas de control.

Este cálculo se realiza de forma automática en la herramienta institucional de gestión de riesgos, considerando la reducción de probabilidad y el impacto, según la efectividad de los controles aplicados.

Para la automatización del cálculo se tuvo en cuenta los siguientes criterios:

- Valor de probabilidad antes de la aplicación de controles.
- Valor de atributos del primer control

Del resultado de la multiplicación de ambos se obtiene el porcentaje que se le resta a la probabilidad inicial, lo cual indica el porcentaje de reducción en probabilidad.

Ejemplo:

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

Valor de probabilidad antes de controles: 60%

Valor de atributos del control 1: 40%

Cálculo de la reducción: 60% x40% = 24%

Este valor se resta de la probabilidad inicial: 60% - 24% = 36%

Dado que en el ejemplo se tenían dos controles, se toma el resultado obtenido del primero control (36%) y de la misma manera se calcula frente al valor de probabilidad y el valor del control. En este sentido, el nivel total de disminución de la probabilidad dependerá del número de controles aplicables.

Se inicia con el último valor de probabilidad dado (36%)

36%*30% = 10.8%

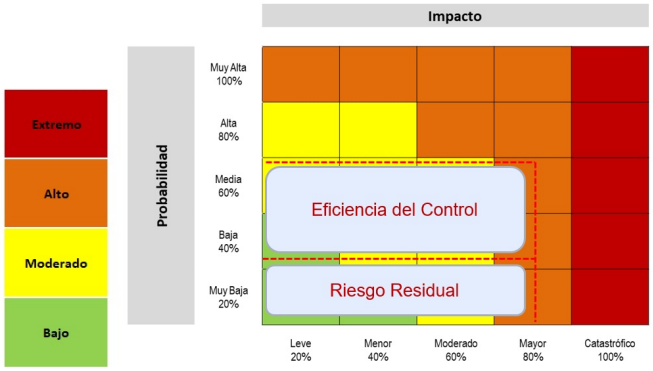
Nuevamente se resta del último valor de probabilidad que es 36%

36% - 10.8% = 25.2%

Como resultado final, la probabilidad de la nueva ubicación en el mapa de calor en un porcentaje de probabilidad de 25.2%

Para los movimientos de impacto, se realizan de la misma manera; sin embargo, se toma como referencia el valor inicial del impacto, en lugar de la probabilidad.

Gráficamente el movimiento en la matriz de calor se muestra en la siguiente imagen:



7.6 Niveles de aceptación del Riesgo

En esta etapa, la entidad define los niveles de aceptación del riesgo de seguridad de la información con base en la valoración del riesgo residual. Los riesgos que en su valoración residual se encuentran en zona de riesgo BAJO, se acepta el riesgo sin que sea necesario documentar acciones inmediatas de tratamiento, manteniendo el seguimiento a los controles establecidos.

Los riesgos cuya valoración residual se encuentren en las zonas: moderado, alto o extremo deberán ser objeto de la definición, aprobación e implementación de un plan de tratamiento del riesgo.

Zona de Riesgo	Descripción
Extremo	Se debe tomar acción inmediata
Alto	Se requiere tomar acciones
Moderado	Se requiere tomar acciones
Bajo	El riesgo es aceptable y no requiere documentar acciones y se realiza seguimiento a los controles definidos

7.7 Tratamiento del riesgo de seguridad de la información

El tratamiento del riesgo corresponde a la respuesta definida por la primera línea de defensa para gestionar los riesgos de seguridad de la información identificados. Para la selección de la opción de tratamiento, los líderes de los procesos deberán considerar la importancia del riesgo, su posible efecto sobre la entidad, la probabilidad de ocurrencia, el impacto asociado y la relación costo-beneficio de las medidas a implementar.

Las opciones de tratamiento del riesgo, se enmarcan en las siguientes categorías:

- Aceptar el Riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.
- Reducir/ Mitigar el Riesgo: Se adoptan medidas para reducir la probabilidad de ocurrencia, o el impacto del riesgo, o ambos, generalmente mediante la implementación de nuevos controles y/o la evaluación de los controles existentes.
- Reducir/ Compartir el Riesgo: Se reduce la probabilidad o el impacto del riesgo mediante su transferencia total o parcial.
- Evitar el Riesgo:Se eliminan las actividades que originan el riesgo, lo cual implica no iniciar o suspender la actividad que lo genera .

Para los riesgos cuya valoración residual se encuentre en las zonas Extremo, Alta o Moderado, se deberán definir planes de tratamiento, seleccionando como opción de tratamiento Reducir/Mitigar el riesgo.

Para el caso de riesgos valorados en zona Baja, el líder del proceso podrá seleccionar la opción:

- Reducir-Mitigar el Riesgo: Formulando acciones para fortalecer o implementar nuevas actividades de control
- Aceptar el Riesgo: No adoptando medidas que afecten la probabilidad y/o impacto.

7.8 Plan de Tratamiento de Riesgos de Seguridad de la Información

El plan de tratamiento de riesgos corresponde al conjunto de acciones específicas definidas para gestionar los riesgos residuales y cuya opción de tratamiento es Reducir-Mitigar el riesgo.

El objetivo del plan de tratamiento es establecer nuevos controles o fortalecer los existentes, mediante ajustes en su diseño, mejoras en su implementación o ampliación de su cobertura.

Las acciones definidas deben registrarse formalmente en el módulo correspondiente de la herramienta institucional de gestión del riesgo y considerar como mínimo los siguientes elementos:

- Acción o Actividad: Es el conjunto de acciones definidas por el proceso orientadas a mitigar o reducir la probabilidad de ocurrencia y el impacto del riesgo residual identificado.
- Responsable: Cargo responsable de garantizar la ejecución del plan de acción en tiempo y forma.
- Fecha de Implementación: Es la fecha a partir de la cual se iniciará la ejecución de la acción definida.
- Responsable de seguimiento: Persona encargada del proceso de Gestión de Tecnologías de realizar el seguimiento a la implementación y cumplimiento de las acciones definidas.

Es responsabilidad del propietario del riesgo, realizar el seguimiento al cumplimiento de los planes de tratamiento del riesgo.

7.9 Aprobación de Riesgos

La aprobación del riesgo de seguridad de la información representa la etapa final del proceso de gestión dentro de la entidad. Este acto formal confirma que los riesgos han sido gestionados y ratifica la responsabilidad asumida por su propietario.

Es importante tener en cuenta que los riesgos aprobados no pueden modificarse ni eliminarse. En caso de requerir ajustes, será necesario volverlos a aprobar en la herramienta institucional de gestión del riesgo.

7.10 Monitoreo y Revisión

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

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

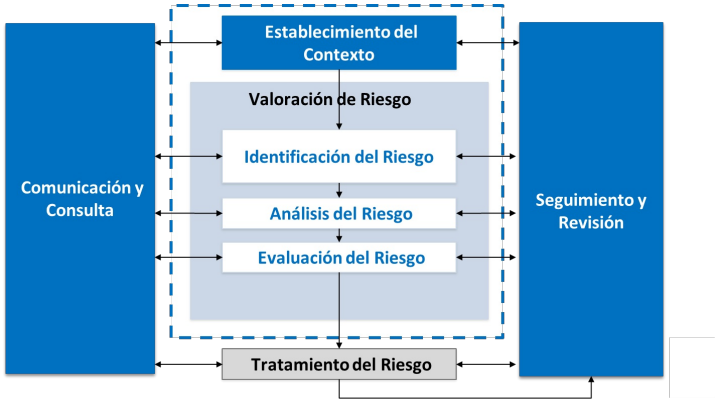
8 METODOLOGÍA PARA LA IDENTIFICACIÓN, EVALUACIÓN Y TRATAMIENTO DE RIESGOS DE CONTINUIDAD DE NEGOCIO

El objetivo de esta metodología es describir el paso a paso para identificar los riesgos potenciales a los que la Secretaría Distrital de Movilidad está expuesta y que podrían causar una interrupción de las operaciones y servicios principales, la valoración de riesgos, así como las medidas que se han adoptado para el tratamiento de los riesgos, para asegurar la continuidad de las operaciones.

Los objetivos específicos son:

- Identificar los riesgos de interrupción de los procesos transversales que podrían alterar la continuidad de sus operaciones.
- Realizar la identificación y clasificación de los controles existentes para la sede de la Calle 13 de Secretaría Distrital de Movilidad.
- Identificar oportunidades de mejora para el fortalecimiento de los controles existentes.

Alineado con el estándar internacional ISO 31000:2009, a continuación, se describen las etapas establecidas en el proceso de gestión de riesgo de continuidad de negocio:



Proceso de gestión para los riesgos de interrupción

La metodología de trabajo incluye el desarrollo de un plan de entrevistas, recorridos a la sede de la calle 13, centros de cómputo y la respuesta a formularios con las y los lideres de cada proceso, orientado a la identificación de riesgos, así como su probabilidad de ocurrencia e impacto estimado.

8.1 Valoración de Riesgo:

Es un proceso general de identificación, análisis y evaluación de riesgos, materializados o potenciales, que pueden conllevar a una interrupción de las operaciones en las sedes incluidas en el estudio.

8.2 Identificación Del Riesgo

En esta etapa del proceso, se busca determinar las fuentes de riesgo, los sucesos, causas y consecuencias, que pueden provocar una interrupción potencial de los procesos críticos de la entidad.

El siguiente esquema, describe los niveles en los que se soporta la misión y operación de la entidad, la capa inferior representa los recursos necesarios para asegurar los procesos y su operación; este esquema permite concentrar la identificación de riesgos de interrupción, en la disponibilidad de los recursos que apoyan la operación misional, dado que su ausencia y afectación podría provocar la interrupción de los procesos críticos de la entidad.

Recursos claves

La identificación de riesgos de interrupción se realiza considerando la no disponibilidad de uno o varios de los recursos claves.

Las técnicas utilizadas para realizar la identificación de los riesgos son entrevistas semiestructuradas con las personas responsables de las áreas transversales, utilizando como herramienta un cuestionario de recopilación de la información creado a partir de los hábitos, de las buenas prácticas, de procedimientos, tecnología e infraestructura, más aceptado y otros extraídos de los estándares internacionales:

- ISO 18001 (Occupational Health and Safety Assessment Specifications
- ISO 27001 (Information Security Management Systems)
- TIA 942 (Telecommunication Infrastructure Standard for Data Centers)
- NFPA 75 (Standard for the Protection of Information Technology Equipment)
- Tier Standard: Topology & Operational Sustainability
- NFPA 1600 (Standard On Disaster/Emergency Management And Business Continuity Programs)
- ISO 22301:2019 y,
- Las buenas prácticas de continuidad de negocio y de recuperación ante desastres del DRI (Disaster Recovery Institute, de Estados Unidos) y el BCI (Business Continuity Institute, del Reino Unido).

El proceso de identificación de riesgos de interrupción consiste en identificar las consecuencias, las fuentes de riesgo y las vulnerabilidades, a partir de la entrevista sostenida con cada uno de los responsables de los procesos transversales, así como las respuestas entregadas por ellos a los cuestionarios.

La técnica de evaluación de estos cuestionarios, en la que siempre se evalúan respuestas cerradas (SI/NO/PARCIAL/N/A), la cual es comparada contra una tabla de respuesta deseable, que sirve como referencia para determinar un nivel adecuado de preparación frente a cada categoría de riesgo; la respuesta a cada pregunta puede ser positiva o negativa (la metodología establece este valor para cada pregunta según el estándar y las mejores prácticas).

A continuación, un ejemplo de uno de los formularios para la identificación de riesgos relacionados con un ausentismo masivo de colaboradores:

Formulario: Identificación RA Recurso Humano (plan emergencia)

Tabla 15. Formulario de identificación de riesgo

PREGUNTA	RESPUESTA - SI - NO	REFERENCIA	INDICADOR	OBSERVACIONES Y/O DESCRIPCIÓN Cómo? Por qué? Cuándo? Qué? Dónde? Quién?
¿Se ha realizado un simulacro de evacuación durante los últimos seis meses?	PARCIAL	SI	Puede existir una amenaza Potencial	Participación en el simulacro Distrital de evacuación en el mes de octubre de 2022, adicional en la sede paloquemao se realizo simulacro de evacuación parcial (primer piso) por simulacro de incendio en el mes de julio 2022.

De acuerdo con la respuesta dada, se puede identificar como una amenaza potencial la falta de orientación o entrenamiento en el plan de emergencia, específicamente en el proceso de evacuación, lo que ante una emergencia podría generar que las y los colaboradores no puedan actuar de tal manera que puedan salvaguardar su integridad física, ocasionando un ausentismo de estos.

La identificación de riesgos se hace por medio de la aplicación de los siguientes formularios:

- Identificación RA Infraestructura Física
- Identificación RA Infraestructura Tecnológica
- Identificación RA Recurso Humano (plan emergencia)
- Identificación RA_Seguridad de la Información

Además, se aplica un formulario por cada proceso crítico con el fin de identificar riesgos de interrupción relacionados con la falla en la prestación de servicio de un proveedor crítico, ausentismo de personal y falla de los servicios de tecnología.

Para cada proceso crítico se identifican y analizan las posibles amenazas y vulnerabilidades que podrían causar una indisponibilidad de algunos de los recursos habilitadores trayendo como consecuencia la interrupción del proceso.

Una amenaza tiene el potencial de causar una indisponibilidad de los recursos habilitadores (Infraestructura física, información, servicios de tecnología, proveedores y colaboradores). Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas, es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. acciones no autorizadas, daño físico, fallas técnicas)

A continuación, se describen una serie de amenazas comunes en continuidad de negocio:

Identificación de Amenazas: Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden materializar los riesgos de interrupción.

A manera de ejemplo se citan las siguientes amenazas:

Tabla de Amenazas Comunes:

Tabla 16. Tabla de amenazas

AMENAZAS MÁS COMUNES	
TIPO	**Descripción de Amenaza**
	Contaminación, Polvo, Corrosión.
	Niveles de temperatura o humedad por fuera de los rangos aceptables.
	Incendio.

Amenazas Físicas	Daño en instalaciones físicas.
	Desastres naturales.
	Asonada/Conmoción civil / Terrorismo/Vandalismo.
	Desastre accidental.
Amenazas Naturales	Fenómeno Sísmico
	Fenómeno meteorológico
	Inundación.
	Fenómeno pandémico/epidémico
Personas	Sobrecarga laboral.
	Ingeniería social.
	Manipulación del hardware
	Manipulación con software
	Acciones fraudulentas
	Tratamiento no autorizado de datos personales
	Entrada no autorizada a las instalaciones
	Uso no autorizado de dispositivos
	Incumplimiento en la disponibilidad del personal
	Uso incorrecto de los dispositivos
	Deterioro de dispositivos o soportes
	Copia fraudulenta de software
	Tratamiento ilegal de datos
	Envío o distribución de malware
	Corrupción de datos
Fallos en la Infraestructura	Fallas de electricidad.
	Fallo de red de telecomunicaciones
	Fallo del equipo de telecomunicaciones
	Fallas en el aire acondicionado.
	Fallas en las UPS.
	Fallas en la planta eléctrica.
	Señales de interferencia.
	Radiación electromagnética
	Daño en componentes tecnológicos
	Falla del equipo

Fallas técnicas	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Amenazas para la organización	Falta de personal
	Falta de recursos
	Fallo de los proveedores de servicios
	Violación de leyes o reglamentos
Fallas de Software	Son errores, defectos o imperfecciones en un programa informático que provocan que no funcione como se esperaba. Estas fallas pueden afectar el comportamiento, el rendimiento, la seguridad o la estabilidad del sistema
Cambio Climático	Modificación significativa y duradera de los patrones climáticos globales o regionales

Vulnerabilidades comunes: La entidad puede identificar vulnerabilidades (debilidades en las siguientes áreas):

- Organización
- Procesos y procedimientos
- Rutinas de gestión
- Personal
- Ambiente físico
- Configuración del sistema de información
- Hardware, software y equipos de comunicaciones
- Dependencia de partes externas

Tabla 17. Tabla de vulnerabilidades

EJEMPLOS DE VULNERABILIDADES
Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento
Ausencia de esquemas de reemplazo periódico
Susceptibilidad a las variaciones de voltaje
Susceptibilidad a las variaciones de temperatura
Almacenamiento sin protección
Falta de cuidado en la disposición final
Copia no controlada
Ausencia o insuficiencia de pruebas de software
Defectos bien conocidos en el software
Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
Configuración incorrecta de parámetros
Ausencia de control de cambios eficaz
Descarga y uso no controlado de software
Ausencia de copias de respaldo
Ausencia de protección física de la edificación, puertas y ventanas
Punto único de fallas
Ausencia de identificación y autentificación de emisor y receptor

Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
Conexiones de red pública sin protección
Ausencia del personal
Uso incorrecto de software y hardware
Falta de conciencia acerca de la seguridad
Ausencia de mecanismos de monitoreo
Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
Ubicación en área susceptible de inundación
Red energética inestable
Ausencia de protección física de la edificación (Puertas y ventanas)
Ausencia de procedimiento formal para el registro y retiro de usuarios
Ausencia de proceso formal para la revisión de los derechos de acceso
Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información
Ausencia de reportes de fallas en los registros de administradores y operadores
Respuesta inadecuada de mantenimiento del servicio
Ausencia de acuerdos de nivel de servicio o insuficiencia de estos
Ausencia de procedimientos de control de cambios
Ausencia de planes de continuidad

En la Imagen a continuación se puede observar un ejemplo de identificación del riesgo de interrupción para el proceso crítico de gestión de trámites y servicios para la ciudadanía.

Tabla 18. Ejemplo de identificación de riesgo de interrupción

Código de riesgo	Proceso Crítico	Amenazas	Vulnerabilidades	Consecuencias	Tipo de Riesgo	Descripción del riesgo
R1	Gestión de Tramites y Servicios para la Ciudadanía	A5- Desastres naturales.	V45 Ausencia de personal	Interrupción de la operación	Riesgo de interrupción	Interrupción de la operación debido a una ausencia de personal por un desastre natural

8.3 Análisis Del Riesgo

La actividad de análisis de riesgo de interrupción consiste en establecer los criterios de riesgo asociados a probabilidad e impacto para cada riesgo de interrupción, así como también la relación existente entre las amenazas potenciales de interrupción y cada uno de los recursos claves, de acuerdo con los escenarios de interrupción establecidos para la entidad.

Figura 57 Escenario de Interrupción

Esta etapa tiene como objetivo establecer los criterios de riesgo asociados a la probabilidad e impacto para cada riesgo de interrupción, así como también la relación existente entre las amenazas potenciales de interrupción y cada uno de los recursos habilitadores, de acuerdo con los escenarios de interrupción que se relacionan a continuación:

Tabla 19. Escenarios de Interrupción para Riesgos de Continuidad de Negocio

ESCENARIOS	DESCRIPCIÓN DEL ESCENARIO	IMPACTOS
Escenarios de Impacto Global	Pandemias, Fenómenos meteorológicos, desaceleración económica global, cambios climáticos, Ciberataques, conflictos políticos globales.	No disponibilidad de la infraestructura física.
Escenarios de Impacto Nacional, Regional o Local	Desastres naturales (como Terremotos, inundaciones, huracanes, Tsunamis), conflictos internos del país, epidemias, endemias, cambios climáticos.	No disponibilidad de los servicios tecnológicos.
Escenarios de Impacto Particular	Ciberataques, inundaciones, incendios, desorden público, manifestaciones, protestas, bloqueos, endemias, fallas en los servicios críticos por parte de los proveedores.	No disponibilidad de información. No disponibilidad de proveedores y/o terceros críticos para el proceso. No disponibilidad de colaboradores del proceso.

Se determina la probabilidad de ocurrencia que pueda tener el riesgo identificado y su impacto en caso de materializarse, esta medición se realiza a través de una tabla de probabilidad y otra de impacto de cinco (5) niveles cada una, el cruce entre la probabilidad y el impacto determinará el riesgo inherente.

Tabla 20. Determinación de la probabilidad para riesgos de Continuidad de Negocio

Nivel	*Frecuencia cualitativa	Cálculo de probabilidad
1	Muy baja probabilidad de que ocurra en el último año	Muy Baja
2	Baja probabilidad de ocurrencia en el último año	Baja
3	Mediana probabilidad de ocurrencia en el último año	Media
4	Significativa probabilidad de ocurrencia en el último año	Alta
5	Casi con certeza se espera la ocurrencia del evento en el último año	Muy Alta

Determinar el impacto: para determinar el impacto se tendrán en cuenta los criterios de la Guía Para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP (reputacional y económico) y adicionalmente los criterios de impacto legal, detención o afectación a otros procesos y el impacto operacional:

Tabla 21. Determinación del Impacto para Riesgo de Continuidad del Negocio

Nivel de impacto	Nivel de impacto	Impacto Económico	Impacto en Imagen, Reputación y Credibilidad	Impacto a los Usuarios	Incumplimiento Legal	Detención o impacto a otros procesos	Impacto Operacional
Leve	1	Afectación menor a 10 SMLMV	No se afecta la imagen, reputación y credibilidad de la Entidad	No se generan impactos a los usuarios	No se genera impacto legal	Si el proceso se detiene, no hay afectación sobre otros procesos	Si el proceso se detiene hasta 15 días o más, no generaría un impacto alto para la SDM
Menor	2	Entre 10 y 50 SMLMV	Se genera un impacto en la imagen, reputación y credibilidad de la Entidad ante los colaboradores	Se impacta a los usuarios incumpliendo con los tiempos establecidos para la respuesta a las solicitudes, tramites, requerimentos de información de entidades públicas	Se generan procesos administrativos	Si el proceso se detiene afecta o detiene a un proceso no misional	Si el proceso se detiene entre 5 y 14 días, generaría un impacto alto para la SDM.
Moderado	3	Entre 50 y 100 SMLMV	Se genera un impacto en la imagen, reputación y credibilidad de la Entidad, ante un solo grupo de interés.	Se impacta la atención a los usuarios generando reclamaciones o quejas por la no prestación oportuna del servicio	Se generan procesos sancionatorios (por incumplimientos normativos, legales o contractuales) y/o disciplinarios	Si el proceso se detiene puede afectar un proceso misional o de apoyo clave	Si el proceso se detiene entre 2 y 4 días, generaría un impacto alto para la SDM.
Mayor	4	Entre 100 y 500 SMLMV	Se genera un impacto en la imagen, reputación y credibilidad de la Entidad, ante dos o más grupos de interés.	Impacto en la atención de alguinos trámites, servicios a los usuarios y requerimentos de información de entidades públicas	Se generan procesos fiscales (podría incluir sancionatorios y/o disciplinarios) o Demandas de usuarios	Si el proceso se detiene, puede detener mas de un proceso misional o de apoyo clave	Si el proceso se detiene hasta por 1 día, se generaría un impacto alto para la SDM.
Catastrófico	5	Mayor a 500 SMLMV	Se genera un impacto en la imagen, reputación y credibilidad de la Entidad, sobre todos los grupos de interés o ante medios de comunicación locales, nacionales y redes sociales	Impacto masivo en la atención de trámites, servicios a todos los usuarios y requerimentos de información a entidades públicas	Se generan procesos penales	Si el proceso se detiene puede afectar o detener toda la cadena de valor de la SDM	Si el proceso se detiene por 8 horas o menos, generaría un impacto alto para la SDM

8.4 Riesgo Inherente:

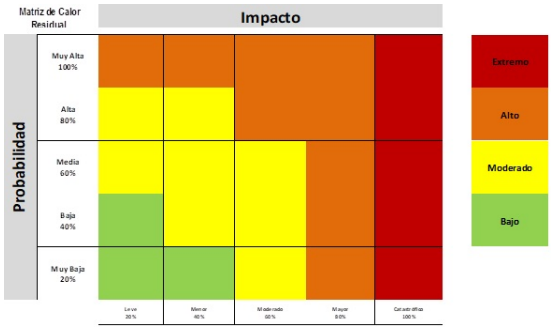


Figura 58 Mapa de Calor de Riesgo Inherente para Riesgo de Continuidad de Negocio

8.5 Etapa de control:

Después de determinado el riesgo inherente, se deben establecer controles de tipo correctivos encaminados a reducir el impacto del riesgo identificado. Para surtir esta etapa se necesita:

- Establecer la estrategia de Continuidad de Negocio
- Determinar los planes de Contingencia y Continuidad de Negocio
- Planear ejercicios de Continuidad
- Desarrollar un programa continuo de capacitación y sensibilización

a. Estrategia BCP: La Estrategia de Continuidad de Negocio, está soportada y documentada en sus Planes de Continuidad de Negocio (BCP) y en el Plan de Recuperación ante Desastres (DRP), los cuales definen el modelo de acción que integrado con una adecuada solución de infraestructura tecnológica, permite a la entidad restablecer las operaciones de misión crítica del negocio, recuperando así la capacidad de operación en un marco de tiempo aceptable y a un nivel predefinido, tras la ocurrencia de un incidente o desastre que impacte a la Secretaria Distrital de Movilidad.

- La Estrategia de Continuidad de Negocio contempla alternativas de recuperación para responder a un incidente de interrupción que afecte la operación de la entidad.
- Cada alternativa de recuperación propuesta está diseñada para cubrir, responder y recuperar el proceso en su momento más crítico.
- Las alternativas de recuperación propuestas son viables y factibles de implementar para cada uno de los procesos críticos de la entidad.
- La presente Estrategia de Continuidad de Negocio se considera funcional al estar implementado el Plan de Recuperación ante Desastres (DRP) y los Planes Alternos de Operación.

b. Planes de Contingencia y Continuidad: a continuación, se relacionan los tipos de planes y su propósito:

- Plan de Manejo de Crisis: establece los parámetros necesarios para tomar decisiones, gestionar, coordinar, evaluar, analizar una crisis, recuperar y mantener las operaciones a un nivel predeterminado en caso de ocurrir una interrupción y un procedimiento básico de comunicaciones a seguir en caso de enfrentar una situación de crisis.
- Planes de Continuidad: definen las acciones y lineamientos a seguir por parte de los equipos de recuperación del proceso crítico, durante y después de un evento de interrupción.
- Planes de Recuperación ante Desastres: definen las acciones y tareas a seguir antes, durante y después de un evento de interrupción, para recuperar los servicios de TI en el Data Center Alterno.
- Plan de Emergencias: Define el actuar ante situaciones de emergencias, con el fin salvaguardar la integridad física de las personas y de las instalaciones físicas.

c. Ejercicios de Continuidad: Consiste en un proceso para entrenar, evaluar, practicar y mejorar el desempeño de una organización" ISO 22301:2019. Es además una herramienta de validación de los planes de continuidad, para asegurar que la estrategia desarrollada es capaz de proveer resultados de respuesta y recuperación ante una interrupción de las operaciones.

Beneficios de los ejercicios:

- Evaluar la factibilidad del plan.
- Practicar los procedimientos antes del evento de interrupción.
- Satisfacer requerimientos legales y de auditoría interna.
- Permitir que el programa BCM permanezca activo, actualizado, entendible y usable.
- Demostrar la capacidad de recuperación.

- Proporcionar un mecanismo para el mantenimiento y actualización del plan.
- Aumentar la capacidad de resiliencia organizacional.

d. Capacitación y sensibilización: Consiste en desarrollar un programa continuo de capacitación y sensibilización a toda la entidad sobre la importancia y los beneficios de contar con planes y estrategias de continuidad de negocio, así como objetivos, política, roles y demás elementos del SGCN.

Los controles en continuidad de negocio son de tipo correctivos, se deben evaluar los atributos para darle formalidad al control y complementar su análisis de acuerdo con la siguiente información:

- Para la calificación se tuvo en cuenta la implementación si era manual o automático, y Acción Oportuna del Control con 3 opciones.
- El 100% se dividió en estas 5 opciones, pero no de igual para todos, de acuerdo al DAFP proporciona valores de % para automático del 25% y manual del 15%, que para el caso fueron los aplicados.
- Para el 60% restante se relaciona a las acciones oportunas del control, de la siguiente manera:

1. No contribuye directamente en la recuperación del proceso crítico afectado - 15%

2. Contribuye parcialmente en la recuperación del proceso crítico afectado - 20%

3. Contribuye directamente en la recuperación del proceso crítico afectado dentro de los tiempos objetivo - 25%

De acuerdo con lo anterior la calificación del control se calcula con la suma de los 2 atributos seleccionados detallados anteriormente.

Características			**Descripción**	**Peso**
Atributos de Eficacia	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
	Acción Oportuna del Control	No contribuye directamente en la recuperación del proceso crítico afectado		15%
		Contribuye parcialmente en la recuperación del proceso crítico afectado		20%
		Contribuye directamente en la recuperación del proceso crítico afectado dentro de los tiempos objetivo		25%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Evidencia	Con Registro	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

A continuación, un ejemplo de un control y su valoración de acuerdo a los atributos relacionados:

Tabla 22. Ejemplo de valoración de controles

Código del Control	Dominio del Control	Descripción de control	Responsable del Control	Tipo		Implementación	Acción Oportuna del Control	Documentación	Evidencia
C1	Controles de personas	Activación de backup o alternos de primer y segundo nivel	Líder del proceso	Correctivo	Correctivo	Manual	Contribuye directamente en la recuperación del proceso crítico afectado dentro de los tiempos objetivo	Documentado	Con registro

8.6 Riesgo Residual:

Como resultado del diseño y análisis de controles, se obtiene el riesgo residual que indicará el desplazamiento del riesgo en el nivel de impacto, de acuerdo con la efectividad del control tal como se muestra a continuación:

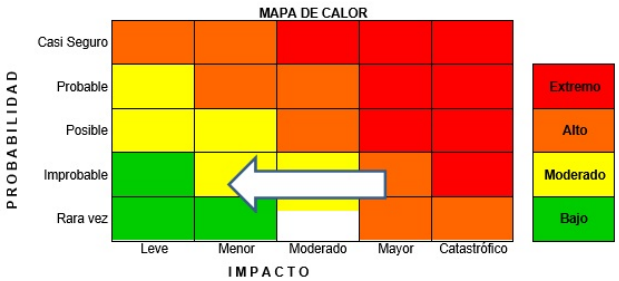


Figura 59 Mapa de calor de riesgo residual para riesgo de continuidad del negocio

Los riesgos residuales de interrupción o de continuidad reducen impacto ya que sus controles son correctivos y se activan únicamente cuando se presentan un incidente de interrupción, como por ejemplo, si se presenta una falla total del centro de computo principal, generando una indisponibilidad de los servicios de tecnología y como consecuencia la interrupción de los procesos críticos de la entidad; se activara el control (Estrategia DRP), es decir se activara y restaurarán los servicios de tecnología críticos desde otro centro de cómputo alterno.

8.7 Tratamiento de los Riesgos:

Definición metodológica de tratamiento del riesgo

El tratamiento del riesgo consiste en la selección e implementación de medidas destinadas a modificar los riesgos identificados, de acuerdo con el apetito de riesgo definido en el marco de continuidad de negocio de la Secretaría Distrital de Movilidad. Las opciones de tratamiento consideradas son:

- **Evitar el riesgo**: eliminar la actividad que lo genera.
- **Reducir o mitigar el riesgo**: implementar controles que disminuyan el impacto del riesgo en caso de materializarse. En el contexto de continuidad de negocio, los controles establecidos están orientados a **reducir el impacto y no la probabilidad** de ocurrencia.
- **Transferir el riesgo**: trasladar total o parcialmente la responsabilidad a un tercero (por ejemplo, seguros o contratos).
- **Aceptar el riesgo**: reconocer el riesgo sin aplicar medidas adicionales, siempre que se encuentre dentro de los límites aceptables.

Criterios de aplicación

- Para **riesgos inherentes moderados y altos**, el tratamiento definido es **reducir o mitigar el riesgo**, en concordancia con el apetito de riesgo institucional en continuidad de negocio.
- Para **riesgos inherentes bajos**, el tratamiento establecido es **aceptar el riesgo**, dado que su impacto potencial se encuentra dentro de los niveles tolerables para la organización

En la siguiente tabla se relacionan los campos a tener en cuenta:

Tabla 23. Ejemplo de Seguimiento y revisión de riesgos de continuidad del negocio

Seguimiento y Medición											
Se presentaron incidentes de interrupción?	Descripción del incidente	Control activado	Fecha de activación del control	El control permitió la recuperación del proceso?	Responsable del control	Se genero un plan de mejora?	Evidencia	Se desarrollo prueba relacionada con el riesgo de interrupción?	La prueba fue exitosa?	Se genero un plan de mejora?	Evidencia

8.8 Etapa de monitoreo:

En esta etapa se lleva a cabo la revisión y actualización de los riesgos de Continuidad de Negocio con periodicidad semestral, con el propósito de identificar cualquier cambio, tomando como base insumos tales como: la respuesta y gestión a incidentes de interrupción o de continuidad, la implementación de nuevos proyectos al interior de la entidad, cambios en la plataforma tecnológica, automatización de procesos, cambios en la normatividad aplicable, informes de auditoría y órganos de control, que puedan dar origen a nuevos riesgos o modificar la medición de probabilidad y/o impacto del riesgo a nivel inherente y/o residual, para ello el Oficial de Continuidad evaluará el indicador de gestión: Gestionar el 80% de los incidentes reportados de interrupción y continuidad de acuerdo a los tiempos establecidos.

Asimismo, la persona Oficial de Continuidad en ejercicio de su rol como segunda línea de defensa, verifica la efectividad de los controles, que para el caso de la gestión de continuidad de negocio corresponde a la(s) estrategia(s) de continuidad de negocio, los planes de continuidad, ejercicios de continuidad, el programa de capacitación y sensibilización dirigido a toda la entidad a través de la evaluación de efectividad de éstas.

Mediante la gestión de los incidentes de interrupción, se analizan aquellos riesgos que se hayan materializado con incidencia en la continuidad de negocio y, con base en los resultados obtenidos de los ejercicios de continuidad de negocio, de las revisiones por la Dirección, del comportamiento de los indicadores de gestión del SGCCN, entre otros.

9 METODOLOGÍA PARA LA IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE LOS RIESGOS PARA EL SISTEMA DE ADMINISTRACIÓN DE RIESGOS DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO - SARLAFT

Introducción

La presente metodología se encuentra articulada con la Guía de administración del riesgo y el diseño de controles en entidades públicas del DAFP versión 7, esto con el fin de tener un mayor alcance y robustez en la gestión de riesgos del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo SARLAFT que tiene implementado la Entidad de acuerdo a los lineamientos Distritales.

Objetivo

Establecer la metodología para la identificación, evaluación y tratamiento de los riesgos de Lavado de Activos y Financiación del Terrorismo que se puedan presentar en las diversas actividades de vinculación o contratación de personas naturales y jurídicas.

9.1 Responsabilidades

Tabla 24. Responsabilidades - lineas de defensa riesgos de SARLAFT

LINEA DE DEFENSA	RESPONSABLE	RESPONSABILIDADES
Línea Estratégica	**Comité Institucional de Gestión y Desempeño – CIGD**	• Revisar el contexto estratégico, plataforma estratégica, el modelo de operación por procesos y la planeación institucional, con el fin de analizar los posibles eventos de riesgos que se puedan materializar en el ejercicio de las funciones de la Entidad. • Establecer y aprobar la Política de Administración del Riesgo para la Secretaría Distrital de Movilidad - SDM. • Analizar el informe de seguimiento a la gestión del riesgo, con el fin de proponer acciones de mejora y gestionar la toma de decisiones.
Primera Línea	Enlaces Dirección de Contratación y Dirección de Talento Humano y/o Líderes de proceso	• Apoyar la implementación de la política para la administración del riesgo. • Revisar e identificar los riesgos asociados a lavado de activos y/o financiación del terrorismo determinados a sus áreas, sedes, procesos y actividades. • Identificar y documentar los controles para evitar la materialización de los riesgos. • Socializar con sus áreas la matriz de riesgos de SARLAFT garantizando la participación de los jefes de las mismas. • Realizar el monitoreo periódico a la matriz de riesgos de SARLAFT para garantizar la aplicación de los controles. • Realizar el reporte periódico y oportuno de las evidencias de cumplimiento de los controles. • Informar al Oficial de Cumplimiento cada vez que se requiera ajustar la matriz de riesgos de SARLAFT de su proceso. • Socializar los informes de seguimiento de la matriz de riesgos de SARLAFT con los dueños de los procesos. • Verificar que las evidencias reportadas estén acordes con las definidas en los controles para la mitigación del riesgo
	Oficial de cumplimiento	• Acompañar metodológicamente a los procesos que aplica SARLAFT en la construcción o actualización de los mapas de riesgos. • Realizar la evaluación de probabilidad e impacto de cada uno de los riesgos de SARLAFT identificados.
		• Definir la metodología para la administración del riesgo, acorde a la normatividad y

Segunda Línea	Oficial de Cumplimiento	lineamientos distritales y nacionales. • Adelantar el monitoreo de los mapas de riesgos, evaluando la eficacia de los controles y los cambios de valoración del riesgo residual que se presenten en el ejercicio de la gestión del riesgo. • Consolidar y publicar los mapas, acorde a los lineamientos normativos • Revisar periódicamente la matriz de riesgos de SARLAFT. • Aprobar la matriz de riesgos de SARLAFT. • Socializar en el Comité Institucional de Gestión y Desempeño la matriz de riesgos de SARLAFT. • Aprobar el plan de tratamiento de riesgos. • Generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas. • Verificar que las evidencias reportadas estén acordes con las definidas en los controles para la mitigación del riesgo.
Tercera Línea	**Oficina de Control Interno - OCI**	• Generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas, a partir de auditorías, seguimientos y/o monitoreos, según actividades programadas en el PAAI aprobado (según selectivo). • Verificar la aplicación metodológica de la guía para la gestión del riesgo en la SDM y la aplicación de la política. • Evaluar la efectividad de los controles y planes de acción propuestos, según selectivo y programación del PAAI aprobado para la vigencia. • Publicar los seguimientos realizados a los mapas de riesgo.

9.2 Metodología riesgos SARLAFT

9.2.1 Identificación del riesgo

La identificación es la etapa donde se analizan los riesgos que están bajo el control de la organización, para la cual se debe tener en cuenta el contexto estratégico en el que opera la entidad, de igual manera el análisis de los factores internos y externos que afecten el cumplimiento de los objetivos institucionales.

a. Análisis de objetivos estratégicos y de los procesos:

Análisis de objetivos estratégicos	**Análisis de objetivos del proceso**
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso, así mismo, los objetivos asociados al sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo - SARLAFT.	Los objetivos de los procesos deben estar alineados con los objetivos estratégicos, así como con la misión, visión y objetivos de SARLAFT.

Cadena de valor

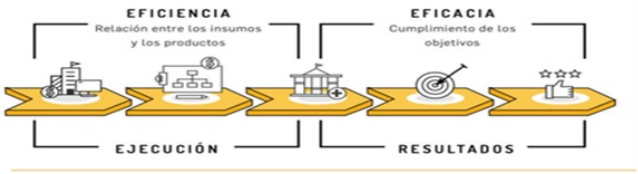


Figura 60 Cadena de valor

Por medio de la cadena de valor se pueden identificar las actividades que están dentro del flujo del proceso y a partir de éstas identificar la posibilidad de presentarse la materialización de un riesgo en el cumplimento de los objetivos del proceso, del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo o de la entidad.

b. **Área de impacto**

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional, para algunos riesgos puede presentarse que la afectación sea de tipo económica y reputacional a la vez.

c. **Áreas de factores de riesgo**

Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

FACTOR	**DESCRIPCION**	**DESCRIPTOR**
Transacción u Operación	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la Entidad (naturales o jurídicas)
		Productos (bienes o servicios) que oferta / requiere
		Canales utilizados para la operación
		Jurisdicciones (nacional o territorial)

d. **Descripción del riesgo**

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

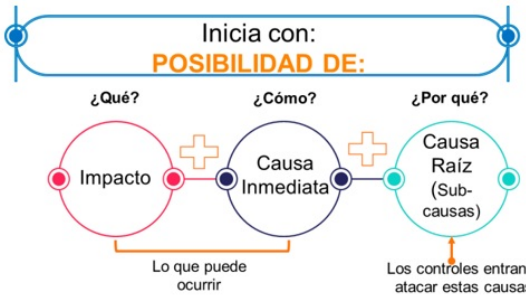


Figura 61 Estructura para la redacción del riesgo

Es importante tener presente que para la redacción de los riesgos SARLAFT se debe: revisar la documentación de los procesos de Gestión de Talento Humano y Gestión Jurídica (Contratación) para identificar riesgos relacionados con el lavado de activos y financiación del terrorismo y los controles, documentar quién es la persona responsable de ejecutar los controles, la periodicidad con que se aplicará, el soporte que quedará como evidencia de la ejecución del mismo y validar que los riesgos identificados correspondan con las actividades propias de los proceso y del área, así mismo, los controles y responsables de los mismos.

Ejemplo:

Redacción inicia con:	**IMPACTO** **¿Qué?**	**CAUSA INMEDIATA** **¿Cómo?**	**CAUSA RAIZ** **¿Por qué?**
Posibilidad de	afectación económica	por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva,	a causa de fallas en las operaciones de pago de subsidios.

Redacción final del riesgo: Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas en las operaciones de pago de subsidios.

Premisas para una adecuada redacción del riesgo:

- No describir como riesgos fallas ni desviaciones del control.
- No describir riesgos como la negación de un control.
- No existen riesgos transversales, lo que pueden existir son causas transversales.

9.2.2 Valoración del riesgo

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

a. **Tabla de probabilidad**: Teniendo en cuenta el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, la cual se describe en la siguiente tabla, que establece los criterios para definir el nivel de probabilidad.

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Figura 62 Criterios para definir el nivel de probabilidad

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

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

Figura 63 Criterios para definir el nivel de impacto

La valoración de riesgos se realizará en conjunto entre el líder y/o el enlace de calidad del proceso y el Oficial de Cumplimiento y/o su delegado, con el fin de mantener la imparcialidad frente a la valoración que se viene manejando desde SARLAFT.

9.2.3. 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 residual (RIESGO INHERENTE).

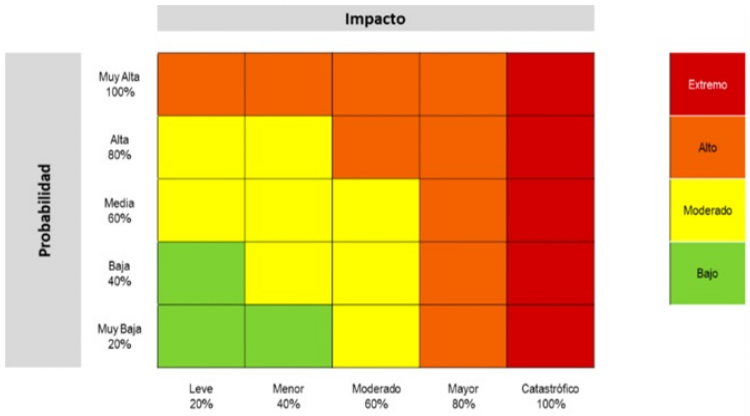


Figura 64 Matriz de calor (niveles de severidad del riesgo)

9.2.4 Valoración de controles

Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer, o a través del análisis de los procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.
- Los responsables de implementar y monitorear los controles son las/los líderes de proceso con el apoyo de su equipo de trabajo

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

- **Responsable de ejecutar el control:** Identifica el cargo de la/el servidor (a) 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.

Figura 65 Estructura para la redacción de controles

Ejemplo:

RESPONSABLE	ACCION	COMPLEMENTO
El profesional de la Dirección de Contratación	verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos al tipo de contratación,	a través de la lista de chequeo de requisitos, se revisa frente a la información suministrada por el proveedor, si este cumple se registra en el sistema de información de contratación.

Redacción final del control: El profesional de la Dirección de Contratación verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos al tipo de contratación, a través de la lista de chequeo de requisitos, se revisa frente a la información suministrada por el proveedor, si este cumple se registra en el sistema de información de contratación.

9.2.5 Tipología de controles

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

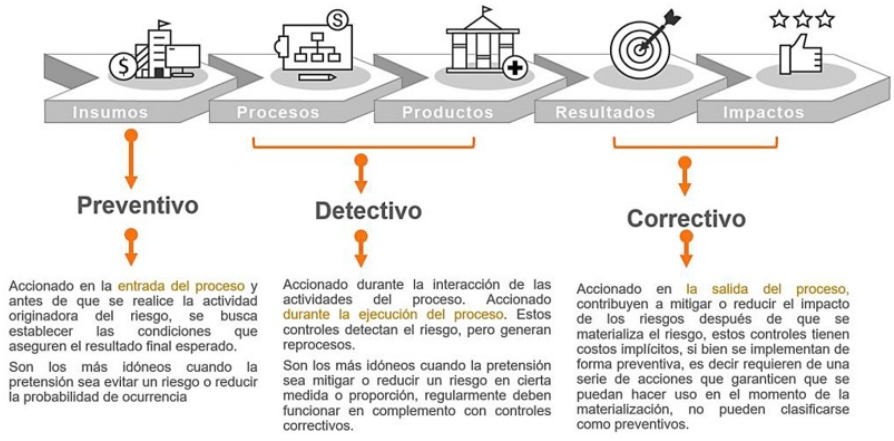


Figura 66 Cadena de valor del proceso y las tipologías de controles

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

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

- **Control manual:** Son ejecutados por personas.
- **Control automático:** Ejecutados por un sistema o software previamente programado o diseñado.

9.2.6 Valoración de controles

A continuación, se analizan los atributos del control:

Tabla 25. Valoración de controles

CARACTERISTICAS DE EFICIENCIA		PESO
TIPO	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
IMPLEMENTACION	Automático	25%
	Manual	15%

Tabla 26. Análisis atributos formalización del control

CARACTERISTICAS DE EFICIENCIA		DESCRIPCIÓN
DOCUMENTACION	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros esquemas	Políticas de operación, manuales o guías específicas.
FRECUENCIA	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral)	
EVIDENCIA (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
EJECUCIÓN (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Los atributos de formalización solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que del valor de los atributos se genera el movimiento del mapa de calor, se debe tener en cuenta los tipos de movimientos dependiendo del tipo de control implementado.

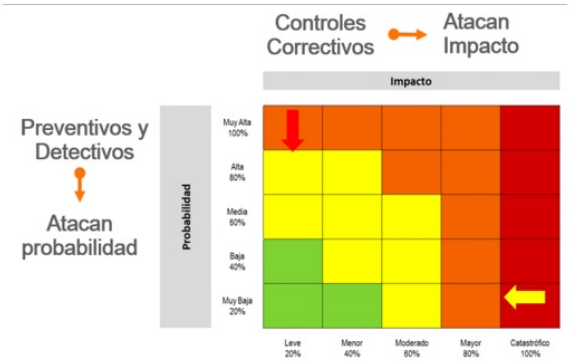


Figura 67 Movimiento en la matriz de calor acorde con el tipo de control

9.3 Valoración de riesgo residual

Con esta información se procede a realizar el cálculo del nivel de riesgo residual de la siguiente manera.

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

Figura 68 Aplicación de controles para establecer el riesgo residual

9.4. Lineamientos y/o políticas de operación

- La matriz de riesgos de SARLAFT será revisada una vez al año con el fin de identificar nuevos riesgos y/o actualizar los controles para cada uno de ellos; a menos que por el estado del proceso o por su nivel de importancia sea necesario hacerlo con mayor frecuencia.
- Esta actualización es responsabilidad del Oficial de Cumplimiento quien, con el apoyo de los enlaces de los procesos involucrados del Equipo Técnico de Calidad, revisará y actualizará el mapa de riesgos de SARLAFT.
- Es necesario que las personas y partes involucradas tanto internas como externas, estén informadas sobre los riesgos a los cuales se encuentran expuestos y que se establezcan los mecanismos de consulta y comunicación con el fin de mantener informados de este proceso.
- Los enlaces de los procesos involucrados del Equipo Técnico de Calidad deberán garantizar que los controles se estén ejecutando conforme se documenten en la matriz, en el caso de algún cambio en estos controles deberá solicitar la actualización al Oficial de Cumplimiento.
- El Oficial de Cumplimiento y/o Equipo SARLAFT realizarán el monitoreo al mapa de riesgos de SARLAFT, con corte al 31 de enero y 31 de julio de cada vigencia, y lo comunicarán y publicarán en la página web de la SDM, en el link de transparencia y acceso a la información pública, para conocimiento de las partes interesadas.
- Producto del seguimiento semestral al mapa de riesgos de SARLAFT el Oficial de Cumplimiento emitirá informe de resultados de la evaluación de los controles y del plan de tratamiento.
- El Oficial de Cumplimiento socializará ante la Alta Dirección los resultados del seguimiento a la matriz de riesgos de SARLAFT mediante memorando.

9.5 Materialización de riesgos de SARLAFT

En el caso de la materialización de un riesgo de SARLAFT se deberá aplicar lo establecido en la política de riesgos de SIGRIP.

10. Lineamientos generales de la guía

- Las actualizaciones a la presente guía se deben socializar en el Comité Institucional de Coordinación de Control Interno - CICCI.
- Cuando se requiera realizar un tema nuevo o actualizar algún capítulo, se debe solicitar por el integrante del Equipo Técnico que lidere la metodología del tema incluir o modificar.
- Las actualizaciones realizadas a la presenta guía serán firmadas únicamente por los responsables de los cambios hechos en la versión correspondiente

ELABORÓ DEL PROCESO	REVISÓ DEL PROCESO	REVISÓ OFICINA ASESORA DE PLANEACIÓN INSTITUCIONAL	APROBÓ
Julio Roberto Fuentes Vidal Contratista 2026-04-29 08:55:53 Sergio Daniel Ramos Alvarez Contratista 2026-04-29 13:40:07 Duvier Moreno Ariza Contratista 2026-04-29 09:01:58 Ismael Daniel Esteban Mateus Velez Contratista 2026-04-29 13:55:23	Duvier Moreno Ariza Contratista 2026-04-29 13:59:24	Julio Roberto Fuentes Vidal Contratista 2026-04-29 15:53:12	Claudia Elena Parada Aponte Profesional Especializado(a) 222-19 2026-04-29 16:26:30 Clemencia Rojas Arias Subsecretario(a) 2026-04-30 08:11:53