ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE MOVILIDAD	
	CÓDIGO:PE01-G01

1. **OBJETIVO GUÍA**

Establecer el marco general para la gestión del riesgo en todos los niveles de la entidad, abarcand trabajo y continuidad del negocio que afecten el cumplimiento de la misionalidad y el logro de sus ob

2. **POLÍTICA DE ADMINISTRACIÓN DEL RIESGO EN LA SDM**

Introducción

La Secretaría Distrital de Movilidad definió su política de administración del riesgo como la expresi gestión realizada por la entidad, en cumplimiento de su misionalidad.

Así mismo, la SDM estableció como marco de referencia el Modelo Integrado de Planeación y G Estratégico y Control Interno, siendo el eje fundamental de análisis el contexto organizacional inte operación por procesos.

Por lo anterior, la entidad busca implementar la gestión del riesgo, fomentando una cultura organiza tomar decisiones oportunamente, en pro de la mejora continua.

Objetivo de la Política

Establecer el marco general para la gestión del riesgo en todos los niveles de la entidad, a través d sistemas de gestión, teniendo en cuenta el contexto interno y externo, el modelo de operación institucionalmente.

Alcance de la Política

La política de riesgos es aplicable para todos los niveles de la entidad, servicios, procesos, program

Términos y Definiciones

Las definidas en el documento “PE01-PR04-F04 Glosario Secretaría Distrital de Movilidad”, entre la

- Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organi
- Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus ob gestionar.
- Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y
- Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pue
- Causa Inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el
- Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede pres una causa o sub-causas que pueden ser analizadas.
- Conflicto de intereses: Situación donde los intereses de negocios, financieros, familiares, políti
- Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impac
- Control: Medida que permite reducir o mitigar un riesgo.
- Debida diligencia: Proceso para evaluar con mayor detalle la naturaleza y alcance del riesgo d
- Factores de Riesgo: Son las fuentes generadoras de riesgos.
- Función de Cumplimiento Antisoborno: Personas con responsabilidad y autoridad para la oper
- Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesg
- Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia
- Programa de Transparencia y Ética Pública PTEP: Plan que contempla la estrategia de lucha
- Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposi año.
- Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potencial la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- Riesgo de Corrupción: Posibilidad que, por acción u omisión, se use el poder para desviar la g
- Riesgo de Soborno: Cualquier situación donde exista una transacción indebida de dinero u c manera ilegal. El riesgo de soborno se compara con otros riesgos del negocio para establecer
- Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilid
- Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.
- Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda exp consecuencias. (ISO/IEC 27000).
- Soborno: Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualqui incentivo o recompensa para que una persona actúe o deje de actuar en relación con el deser
- Socio de negocio: Parte externa con la que la organización tiene, o planifica establecer, algún
- Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con res

Contexto Organizacional

Como parte del análisis de contexto de la Secretaría Distrital de Movilidad, se documenta en la mat del software MIPG utilizado por la entidad, en el primer trimestre de cada vigencia.

Adicionalmente en el documento “Caracterización de usuarios y partes interesadas”, se consolidan en el marco del Modelo Integrado de Planeación y Gestión MIPG

En lo que respecta a los riesgos de corrupción la entidad debe evaluar la información proveniente q

La entidad debe incluir en la política los resultados de las evaluaciones llevadas a cabo por los orga

Roles y Responsabilidades

Para la adecuada gestión del riesgo la Secretaría Distrital de Movilidad, define los roles y responsab

a. Comité Institucional de Gestión y Desempeño – CIGD.

- Revisar el contexto estratégico, plataforma estratégica, el modelo de operación por procesos y
- Establecer y aprobar la Política de Administración del Riesgo para la Secretaría de Movilidad.
- Analizar el informe de seguimiento a la gestión del riesgo, con el fin de proponer acciones de r

b. Comité Institucional de Coordinación de Control Interno.

- Fomentar la divulgación, implementación y monitoreo del cumplimiento de la política de admin
- Promover la identificación y análisis del riesgo desde el direccionamiento o planeación estraté
- Monitorear el estado de los riesgos aceptados (apetito del riesgo) con el fin de identificar camb
- Monitorear el seguimiento a la gestión del riesgo por parte de las instancias responsables.
- Fomentar los espacios de capacitación a los líderes de los procesos y sus equipos de trabajo
- Fomentar la generación de acciones para apoyar a la segunda línea de defensa frente al segu

c. Líderes de proceso (primera línea de defensa)

- Liderar la identificación de los riesgos del proceso a cargo, acorde a los lineamientos establec
- En conjunto con el grupo de trabajo, analizar y controlar los riesgos identificados, así mismo re
- Reportar el mapa de riesgos en los tiempos definidos para la entidad, y garantizar el cargue co
- Evaluar periódicamente la eficacia de los controles definidos en la matriz de riesgos del proces
- Reportar los planes de tratamiento en los casos de materialización del riesgo.
- Garantizar los ejercicios de autocontrol, estableciendo la periodicidad y evidencias que soporte

d. Equipo técnico del proceso

- Apoyar la implementación de la presente política para la administración del riesgo.
- Apoyar en la construcción del mapa de riesgos del proceso, acorde con los lineamientos entre
- Socializar al interior del proceso los aspectos relevantes para la administración del riesgo, así
- Realizar ejercicios de autocontrol, estableciendo la periodicidad y evidencias que soporten su

e. Oficina Asesora de Planeación Institucional (Segunda Línea de defensa)

- Definir la metodología para la administración del riesgo, acorde a la normatividad y lineamient de seguridad y salud en el trabajo)
- Adelantar el monitoreo de los mapas de riesgos, evaluando la eficacia de los controles y los ca
- Acompañar metodológicamente a los procesos en la construcción o actualización de los mapa
- Consolidar y publicar los mapas, acorde a los lineamientos normativos

f. Dirección de contratación (Segunda Línea de defensa)

- Monitorear la gestión contractual y generar alertas sobre retrasos, incumplimientos u otras situ

g. Dirección de atención al ciudadano (Segunda Línea de defensa)

- Hacer monitoreo a las PQRD generando alertas sobre incumplimientos, quejas en la prestació

h. Dirección de Talento Humano (Segunda Línea de defensa)

- Monitorear temas clave del ciclo del servidor (PIC, bienestar, incentivos, convivencia laboral, c

i. Oficina de tecnologías de la información y las comunicaciones (Segunda Línea de defensa)

- Monitorear el plan estratégico de tecnologías de la información PETI, generando alertas sobre

j. Dirección de Representación Judicial (Segunda Línea de defensa)

- Monitorear la gestión judicial, generando alertas sobre retrasos, incumplimientos u otras situac

k. Secretaría de despacho, Subsecretarios, Directores, subdirectores y Jefes de Oficina (Segund

- Monitorear aspectos estructurales de los temas bajo su gestión, generando alertas sobre retra

l. Oficial de seguridad de la información (Segunda Línea de defensa)

- Evaluar el cumplimiento de los controles asociados a las Políticas de Seguridad de la Informac

m. Jefe Oficina Asesora de Planeación Institucional, líderes de sistemas de gestión y/o procesos

- Para la evaluación de gestión del riesgo, realizada por la segunda línea de defensa, se debe c

Aspecto a considerar
Las evaluaciones para monitorear el estado de los componentes del sistema de control interno
El cumplimiento legal y obligatorio
Informes a la alta dirección sobre el monitoreo llevado a cabo a los indicadores de gestión, determ
La confiabilidad de la información financiera y no financiera
Informes sobre las deficiencias de los controles a las instancias correspondientes
El acompañamiento a las instancias correspondientes, en la formulación e implementación de las
Cumplimiento de la gestión presupuestal de acuerdo con el marco normativo y la programación in

n. Oficina de Control Interno (tercera línea de defensa)

- Generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas, a pa
- Adelantar el seguimiento a los mapas de riesgos, verificando el adecuado análisis, identificaci
- Verificar que las evidencias reportadas estén acordes con las definidas en los controles para la
- Revisar la efectividad de los controles y planes de acción propuestas, así como de ser necesa
- Solicitar de ser necesario los cambios identificados en pro de la mejora del proceso.

- Publicar los seguimientos realizados a los mapas de riesgo.

Reporte, Monitoreo y Seguimiento de los mapas de riesgos:

Reporte Procesos (Primera línea de defensa)

Mapa de riesgos de corrupción: a corte 30 de abril, agosto 31 y diciembre 31 la primera línea

Para esto, los procesos deberán preparar los reportes de mapas de riesgos 4 días hábiles previos a

Las evidencias serán cargadas con la fecha de corte en los medios definidos por la segunda línea, a veracidad con los datos y soportes cargados.

Mapa de riesgos de gestión: A corte a 30 de junio y diciembre 31 la primera línea de defensa (

Para esto, los procesos deberán preparar los reportes de mapas de riesgos 4 días hábiles previos a

Las evidencias serán cargadas con la fecha de corte en los medios definidos por la segunda línea veracidad con los datos y soportes cargados.

Monitoreo Oficina Asesora de Planeación Institucional (Segunda línea de defensa)

La Oficina Asesora de Planeación Institucional una vez reciba la información del reporte de la ejec publicará los respectivos resultados del monitoreo en el espacio destinado en la página web.

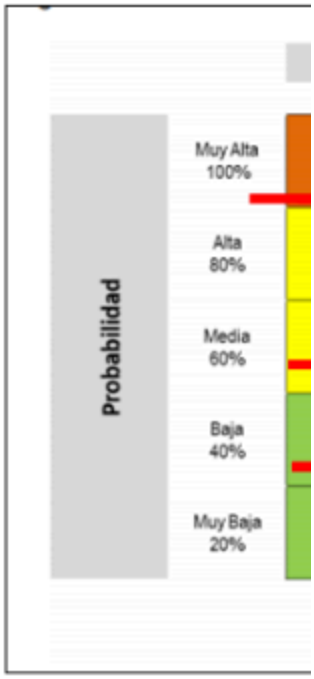
Seguimiento Oficina de Control Interno (Tercera línea de defensa)

Una vez la Oficina Asesora de Planeación Institucional realice el proceso de monitoreo a los ma seguimiento y verificación a la efectividad de los controles, así como, la respectiva publicación del ir

Apetito del riesgo

El apetito del riesgo se define a partir del análisis del nivel del riesgo, el cual se realiza una vez se h

En la Secretaría Distrital de Movilidad se fija el apetito del riesgo, es decir el nivel de riesgos que la desarrollo de sus actividades (Capacidad del riesgo) y por último se analizan los niveles mínimos de



Como se observa el apetito del riesgo deseado para el cumplimiento de los objetivos institucionale teniendo en cuenta que en la memoria histórica de la entidad los niveles de riesgo de la matriz de ca

Para los riesgos de corrupción no es posible aceptar algún nivel de riesgo, su tratamiento siempre e

Escenarios de pérdida de continuidad de negocio

Los procesos analizarán los riesgos asociados con la continuidad de negocio, es decir verificarán si

Escenario	Desc
Colapso de infraestructura física	Imposibilidad de acceso o abandono súbito de las instalacion
Desastre Tecnológico	Pérdida total de la capacidad tecnológica o de los procesos ir
Pandemia	Crisis sanitaria que impide el funcionamiento de los procesos

Materialización del riesgo (Gestión y corrupción)

Riesgos de gestión:

- Informar a la Oficina Asesora de Planeación Institucional como segunda línea de defensa, el e
- Analizar el adecuado cumplimiento de controles, en caso del no cumplimiento se deberá rea modificar, cambiar y/o fortalecer.
- Una vez realizado los respectivos análisis se procederá a ajustar el mapa de riesgos, actualiza
- Cuando se realice el seguimiento cuatrimestral se deberá registrar en el reporte la materializac

Riesgos de corrupción o fraude:

- Activar el plan de contingencia definido en el mapa de riesgos de corrupción para cada riesgo
- Informar a la Oficina Asesora de Planeación Institucional como segunda línea de defensa, el e
- Analizar el adecuado cumplimiento de controles, en caso del no cumplimiento se deberá rea modificar, cambiar y/o fortalecer.
- Una vez realizado los respectivos análisis se procederá a ajustar el mapa de riesgos, actualiza
- Cuando se realice el seguimiento cuatrimestral se deberá registrar en el reporte la materializac

Como insumos se puede tomar la fuente de información de posible materialización del riesgo

- Mesa de ayuda de tecnología a nivel interno
- Información del área o proceso de atención al usuario Las PQRD (peticiones, quejas, reclamo
- Oficina jurídica Líneas internas de denuncia

Eventos de riesgos no identificados

Primera línea de defensa: esta línea de defensa les corresponde a los servidores en sus diferente un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controle consiguiente, identifica, evalúa, controla, mitiga los riesgos.

Adicionalmente, informa a la segunda línea los eventos nuevos que generen un riesgo al cumplimie

Por parte de la segunda línea de defensa: En el momento que se informe de un evento no ident sido identificados en los mapas de riesgo, así como su respectiva actualización y publicación.

Nota: La Entidad dispone de un software como herramienta tecnológica para el cargue y reporte de

2.1 RIESGOS DE GESTIÓN - METODOLOGÍA DEL DEPARTAMENTO ADMINISTRATIVO DE LA

2.1.1Metodología riesgos de gestión

2.1.1.1 Identificación del riesgo

La identificación es la etapa donde se analizan los riesgos que están bajo el control de la organizac cumplimiento de los objetivos institucionales.

a. Análisis de objetivos estratégicos y de los procesos:

Análisis de objetivos estratégicos
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su fracaso

Cadena de valor

Por medio de la cadena de valor se pueden identificar las actividades que están dentro del flujo del

b. **Área de impacto**

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entida
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 fáci
frase “POSIBILIDAD DE” y se analizan los siguientes aspectos:

Ejemplo:

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad

Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan an
para la redacción del riesgo, se tiene:

Redacción final del riesgo: Afectación económica por multa y sanción del ente regulador debido a ac

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: Eje
eventos externos.

Una vez se tenga toda la información, se tiene la primera parte para la construcción del mapa de rie

2.1.1.2 Valoración del riesgo

Establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia e impacto, con el fin d

a. Tabla de probabilidad: Teniendo en cuenta el nivel de probabilidad, la exposición al riesgo esta
la siguiente tabla, que establece los criterios para definir el nivel de probabilidad.

b. Tabla de impacto: En esta tabla se definen los impactos económicos y reputacionales como la

Frente al análisis de probabilidad e impacto no se utiliza el criterio experto, esto quiere decir que el l

Ejemplo (continuación):

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador deb

N.º de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el me

Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 500

2.1.1.3 Evaluación del riesgo

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se

2.1.1.4 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 las
- Los responsables de implementar y monitorear los controles son las/los líderes de proceso co
- Estructura para la descripción del control: Para una adecuada redacción del control se propon
- Responsable de ejecutar el control: Identifica el cargo de la/el servidor (a) que ejecuta el contr
- Acción: Se determina mediante verbos que indican la acción que deben realizar como parte de
- Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del co

2.1.1.5 Tipología de controles

A través del ciclo de los procesos es posible establecer cuando se activa un control, y por lo tanto es

- Control preventivo: control accionado en la entrada del proceso y antes de que se realice la ac
- Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan
- Control correctivo: control accionado en la salida del proceso y después de que se materializa

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

2.1.1.6 Análisis y evaluación de controles

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

Características	Descripción

Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.
		Detectivo	Detecta que algo ocurre y devuelv el proceso a los controles preventivos. Se pueden generar reprocesos.
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.
	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.
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.

***Atributos de Formalización**	Documentación	Documentado	Controles que están documentado 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

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entor

Teniendo en cuenta que del valor de los atributos se genera el movimiento del mapa de calor, se de

Ejemplo:

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador deb

Probabilidad Inherente= moderada 60%

Impacto Inherente: mayor 80%

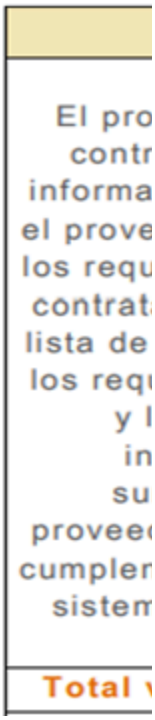
Zona de riesgo: alta

Controles identificados:

Control 1: La/el profesional del área de contratos verifica que la información suministrada por el prov información física suministrada por el proveedor, 48 los contratos que cumplen son registrados en e

Control 2: La/el jefe del área de contratos verifica en el sistema de información de contratación la inf en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Aplicación de atributos según la información del ejemplo:

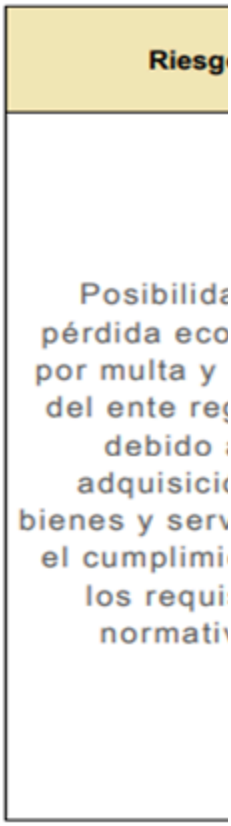

El pro
contr
informa
el prove
los requ
contrat
lista de
los requ
y l
in
su
provee
cumpler
sistem
Total

Como se observa se evalua en el control 1 los atributos en cuanto al tipo de control (preventivo) cor

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

2.1.1.7 Nivel de riesgo residual

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



Acorde a la información de cada control y su valoración en los atributos, se procede a realizar una c

- 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 probabilida

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

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 porce

Para los movimientos de impacto se realizan de la misma manera teniendo como referencia no la pr

En la siguiente tabla se encuentra un resumen del ejercicio de ejemplo hasta la valoración del riesg

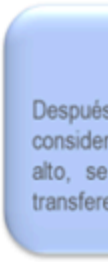
Proceso:	Gestión de re		
Objetivo:	Adquirir con		
Alcance:	Inicia con el requeridas ba		
Referencia	**Impacto**	**Causa inmediata**	
1	Afectación económica	Multa y sanción del organismo de control	

A continuación se aprecia la evaluación del control del ejemplo dentro del mapa de riesgos y su com

No. control	**Descripció**
1	El profesional del verifica que la inf suministrada por corresponda con establecidos de c través de una list donde están los r información y la r información física el proveedor, los cumplen son regis sistema de inform contratación.

2.1.1.8 Estrategias para combatir el riesgo

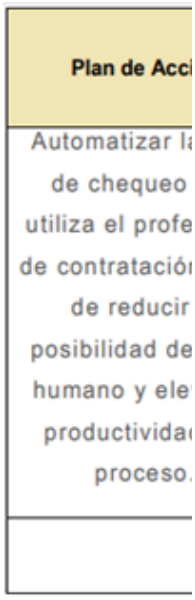
Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, rec



Después
considera
tercerizar
riesgo a tr
La respon
sobre el te
la respon
reputacion

Para la política de tratamiento Reducir mitigar se genera un plan de acción, el cual debe ser diferent

Ejemplo:



2.1.1.9 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 ges
naturaleza pública, a causa de un evento potencial)

Para la identificación, valoración y diseño de controles para los riesgos de tipo fiscal es indispensa
manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adju
patrimonio público

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. Para tener clar
modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio
respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

Control multimodal: Es la articulación entre el sistema de control interno (primer nivel de control) y

Control fiscal interno: Primer nivel para la vigilancia fiscal de los recursos públicos y para la pr
servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniale
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
corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y
la prevención de responsabilidades.

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía,

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a c

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 patrimc

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona co
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 c 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 d de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la pl

Identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las cir gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotació

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, a

Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta múltiples circunstancias inmediatas.

Ahora bien, para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomien el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades 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 l definición de gestión fiscal).

Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgo presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallo responsabilidad fiscal en firme relacionados con hechos de la entidad o del se las advertencias de la Contraloría General de la República y/o las alertas repo el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se r consultar los hallazgos con presunta incidencia fiscal y los fallos con responsa fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años advertencias que se hayan emitido en relación con la gestión fiscal de la entid 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 Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, se puede acceder mediante solicitud de información y documentos (derecho d petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva sector que esta pertenece. Estos precedentes son muy importantes para cono causas raíz (hechos generadores) por los que se ha fallado con responsabilid últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o patrimoniales del Estado. Nota 4: La organización y agrupación por procesos mapa de procesos de la entidad) de los hallazgos con presunta incidencia fisc identificados por el ente de control fiscal, los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector, las advertencias de la Co General de la República y las alertas reportadas en el Sistema de Alertas de Interno -SACI-, es una labor de la segunda línea de defensa, específicamente Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina Interno o quien haga sus veces.
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los h fiscales identificados por el ente de control fiscal y/o de los fallos con respons fiscal relacionados con hechos de la entidad o del sector y/o las advertencias oficina de control interno, en los últimos 3 años? Nota: Se recomienda no cop causas escritas por el órgano de control en el hallazgo, salvo que luego del an propio la entidad concluya que la causa del hallazgo es la identificada por el ó control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del “¿Catálogo Indic Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” son aplic entidad?

Identificación de áreas de impacto:

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscale

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 acc 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 ident de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de nat

Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría ur

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación esta tal.

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es import

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hech 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, ger 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 moratorio

¿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

Descripción del Riesgo Fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los 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 recu
- Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se pre
- Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse

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

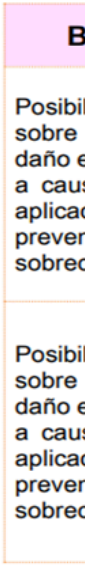
Ejemplo:

Proceso: Gestión de Recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia log

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servic
de recursos.

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, se
naturaleza pública.



Valoración del riesgo fiscal

Evaluación de riesgos: Se busca establecer la probabilidad inherente de ocurrencia del riesgo fisc

Probabilidad: La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según a
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 ec

Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales púb
potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la siguiente tabla definida en

En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que pa
riesgo tiene un nivel de impacto catastrófico

La valoración y el diseño de controles de igual manera se realizan teniendo en cuenta los lineamier

La evaluación del control se realiza de la siguiente manera:

Id Referencia	*Ac*
1	
2	
3	De l
4	
5	Op re
6	C

Id Referencia	Ac
7	Av
8	C
9	Su
10	
11	I
12	e
13	
14	
15	
16	S

Id Referencia	*Ac*
17	
18	
19	
20	
21	Su c r
22	
23	C b
24	M
25	Gir

Id Referencia	Ac
26	Gir
27	R
28	F
29	Fi
30	Fi
31	c
32	
33	P
34	
35	
36	

Id Referencia	Ac
37	Pa
38	
39	
40	
41	
42	B
43	
43	Re
44	
45	

Id Referencia	Ac
46	
47	
48	
49	
50	

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 re

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 materializad

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 r
- **Controles Detectivos** (Detecta que algo ocurre y devuelve el proceso a los controles preventi
- **Controles Correctivos** (Atacan el impacto frente a la materialización del riesgo)

2.2 RIESGOS DE CORRUPCIÓN BAJO LA METODOLOGÍA DEL DEPARTAMENTO DE FUNCIÓ

El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüed

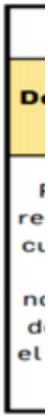
2.2.1 Identificación del riesgo de corrupción o fraude

Las preguntas clave para la identificación del riesgo son:

- ¿Qué puede suceder?
- ¿Cómo puede suceder?
- ¿Cuándo puede suceder?
- ¿Qué consecuencias tendría su materialización?

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



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

- Falta de controles internos y externos efectivos en los procesos y procedimientos, necesarios
- Fallas éticas y de compromiso con lo público que afectan un desarrollo objetivo e imparcial en
- Factores internos que afectan las conductas de integridad pública y propician riesgos de corru
- Factores internos que afectan las conductas de integridad pública y propician riesgos de corru

De igual manera se debe tener en cuenta las siguientes causas para la identificación de los riesgos

- Procesos que involucran trámites que implican manejo de dinero en efectivo
- Falta de segregación de funciones por restricciones de planta Discrecionalidad para la gestión
- Arqueos de caja adelantados por personal no idóneo y sin la autoridad requerida (adelantada
- Gestión Documental con fondos acumulados que no garantizan los registros y memoria institu
- Fases de análisis de los requisitos con excesiva reserva que impida la transparencia en deterr
- Fallas en el apoyo jurídico interno que generan interpretación subjetiva de las normas o reglan
- Factores externos de presión en temas regulados que pueden incidir en las decisiones instituc
- Servidores con conflictos de interés en los temas sobre los cuales pueden incidir con su toma
- Falta de inclusión de acuerdos de confidencialidad y manejo de información interna que facilita
- Falta de herramientas tecnológicas para la transmisión de datos e información entre procesos
- Inexistencia de archivos contables
- Discrecionalidad para la toma de decisiones en grupos restringidos de servidores Ausencia o
- Ausencia de sistemas de información, que pueden facilitar el acceso a información y su posibl

a)Análisis del contexto:

De la misma manera que con los riesgos de gestión, se debe analizar la cadena de valor del proces

C O N T E X T O EXTERNO

C O N T E X T O INTERNO

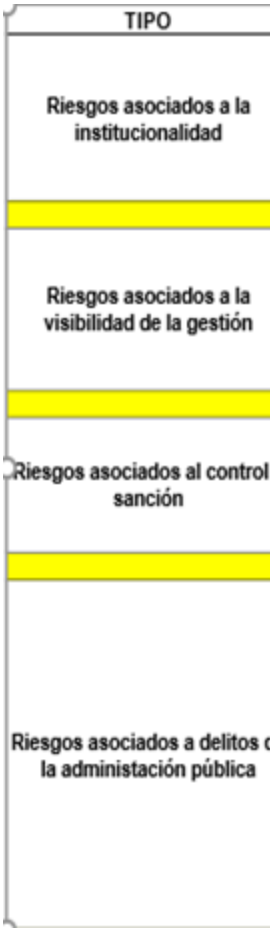
b)Descripción del evento potencial

Evitar iniciar con palabras negativas como: "No.…", "Que no…" o con palabras que denoten un facto

Al evento potencial se le asignan las posibles causas y consecuencias asociadas, se aclara que las

c)Clasificación del riesgo

Acorde a las siguientes tipologías se asocia el riesgo teniendo en cuenta lo relacionado en el siguie



Con la información se tendría la primera etapa de la identificación de riesgos de corrupción como lo

2.2.2 Valoración del riesgo

La valoración del riesgo inherente se realiza basados en la tabla de probabilidad y la tabla de impac

- Tabla de probabilidad: La probabilidad está sujeta a la frecuencia en la que se manifiesta el po

- **Tabla de impacto: Para el análisis del impacto el proceso deberá diligenciar la presente**

N°	
1	¿
2	¿
3	¿

4	¿A en
5	¿C
6	¿C
7	¿A
8	¿E de
9	¿C
10	¿C
11	¿E
12	¿E
13	¿E
14	¿E
15	¿C
16	¿C
17	¿A
18	¿A
19	¿C

Responder afirmati Responder afirmati Responder afirmati catastrófico.	
MODERADO	G
MAYOR	G

Una vez se cuente con la encuesta diligenciada, se procede a verificar el intervalo en donde se encu

2.2.3 Riesgo Inherente:

De igual manera que con el riesgo de gestión, se cuenta con un mapa de calor para el análisis de ni un nivel de riesgo bajo.

2.2.4. Valoración de controles

La valoración de controles se realiza acorde con los parámetros señalados en la versión 4.0 de la G

La redacción del control debe cumplir 6 pasos relacionados en la siguiente tabla:

Una vez se tenga definido y redactado el control, se debe evaluar acorde a las siguientes preguntas

Esta información va a ser clave en el momento de evaluar el control, el diseño del control, la solidez

Calificación del dise
del control

Esta casilla suma
automáticamente la
variables de diseño
6, sin la 7 de evide

De la siguiente manera se puede conocer qué tan bien diseñados se encuentran los controles y su e

Fuerte Diseño fuerte + Eje fuerte No requiere accion fortalecer el control

Y por último después del anterior análisis se determina el número de movimientos en el mapa de ca

2.2.5 Atributos del control

La metodología establece dos tipos de atributos para los controles:

- Detectivos: Son los que se realizan durante la ejecución de la actividad
- Preventivos: Son ejecutados previos a la ejecución de la actividad

Para los riegos de corrupción no se relacionan los controles de tipo preventivo puesto que por su na

Con esto tenemos la segunda fase de contrucción del mapa de riesgos de corrupción como lo refleja

2.2.6 Política de tratamiento del riesgo de corrupción

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes establezca la política de administración del riesgo, las/los dueños de los procesos tendrán en cuen tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que su evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las sig

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a preve entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.

Otras estrategias se encaminan a la sensibilización, comunicación, asesorías, acompañamiento, el

ACCIONES ADICIO
Son acciones comp controles, se debe de ejecución, la fre no son por cada co mitigación del riesg

3 RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO METODOLOGÍA GUÍA TÉCNICA COLO

La metodología adoptada por la Secretaría Distrital de Movilidad para la identificación de peligros, e

en la Guía Técnica Colombiana- GTC 45. 2012-06-20, Guía para la Identificación de los Peligros y l proceso de gestión del riesgo desarrollado en la norma BS 8800 (British Standard) y la NTP 330 del

3.1 Los aspectos para tener en cuenta al desarrollar la identificación de los peligros y la evalu

- Actividades rutinarias y no rutinarias
- Actividades de todas las personas que tienen acceso al sitio de trabajo (incluyendo a contratis
- Peligros identificados que se originan fuera del lugar del trabajo con capacidad de afectar adv
- Los peligros generados en la vecindad del lugar de trabajo por actividades relacionadas con e
- Infraestructura equipo y materiales en lugar de trabajo ya sean suministradas por la Entidad o
- 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
- Cualquier obligación legal aplicable relacionada con la valoración del riesgo y la implementaci
- El diseño del área del trabajo, procesos, instalaciones, maquinarias/equipos, procedimientos c

3.2 Actividades para identificar los peligros y valorar los riesgos

Las siguientes actividades son necesarias para que la SDM, realice la identificación de los peligr

a)La Matriz de identificación de peligros, valoración de riesgos y determinación de controles, se estr 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

c)Clasificar los procesos, las actividades y las tareas: definición de los procesos de trabajo y de cad

d)Identificar los peligros: incluir todos aquellos relacionados con cada actividad laboral. Considerar

e)Identificar los controles existentes: relacionar todos los controles que la SDM ha implementado pa

f)Valorar riesgo:

- Evaluar el riesgo: calificar el riesgo asociado a cada peligro, incluyendo los controles existente
- 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 cont
- Elaborar el plan de acción para el control de los riesgos, con el fin de mejorar los controles exi
- Revisar la conveniencia del plan de acción: revalorar los riesgos con base en los controles pro
- 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 ac

c)Se documenta el seguimiento a la implementación de los controles establecidos en el plan de acc

3.3 EXPLICACION DE LA METODOLOGÍA

La metodología establecida permite realizar un proceso sistemático de identificación de peligros, su

Los pasos básicos a seguir:

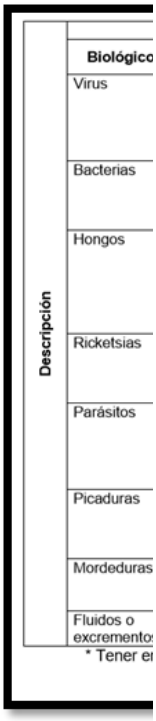
3.3.1 Contexto de la organización.

Implica recolectar la información necesaria para poder adelantar una amplia y completa identificació estratégica, organigrama, información sociodemográfica, tipos de contratación, ubicación geográfica

3.3.2 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



3.3.2.1 Efectos Posibles

Existen efectos que reflejan consecuencias de cada peligro identificado, es decir que se debe tener

lgualmente 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	
Salud	Molestias de cabeza que produ diarrea)

Seguridad	Lesiones poca profundid del ojo po

3.4 Identificación de los Controles Existentes

Se debe identificar los controles existentes y relacionar todos los controles que la Entidad ha implen

- 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 dismi

3.5 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.

3.6 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.

3.7 Evaluación de los riesgos

La evaluación de los riesgos corresponde al proceso de determinar la probabilidad de que ocurran e

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 I
Muy Alto (MA	10
Alto (A)	6
Medio (M)	2
Bajo (B)	No se Asigna Va

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
Frecuente (EF)	3	La situación de exposición se presenta varias veces durante la jorn
Ocasional (EO)	2	La situación de exposición se presenta alguna vez durante la jornac
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 ex 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 contin 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 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 (Incapacic
Grave (G)	25	Lesiones o enfermedades con incapacidad laboral tempo
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 má

Los resultados de las Tablas 5 y 6 se combinan en la Tabla 7 para obtener el nivel de riesgo, el cual

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 – 2 50**	**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.

3.8 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 establecer cuáles categorías son aceptables y cuáles no.

Para hacer esto, la Entidad debe primero establecer los criterios de aceptabilidad, con el fin de prop 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

La exposición al riesgo individual de los miembros de los grupos especiales también se debe consic

3.9 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 me

El resultado de una valoración de los riesgos debería incluir un inventario de acciones, en orden de

3.10 Criterios para establecer controles

Si existe una identificación de los peligros y valoración de los riegos en forma detallada es mucho
tres (3) criterios:

Número de expuestos: Número de personal involucrado en ese Grupo a área de trabajo tanto de pla

Peor consecuencia: Se determinará el mayor efecto posible en la salud del trabajador. Ejemplo: Exp
Intoxicación sistémica, Efectos asfixiantes y/o Muerte. (Estas ya se encuentran por cada Peligro en

Existe requisito legal específico asociado: La Entidad establece si existe o no un requisito legal espe

3.11 Medidas de intervención

Una vez completada la valoración de los riesgos, la Entidad deberá estar en capacidad de determin
controles de ingeniería, controles administrativos o equipos y elementos de protección.

Eliminación: "Modificar un diseño para eliminar el peligro, por ejemplo, introducir dispositivos mec
(Definición Decreto 1072/2015)"

Sustitución: "Reemplazar por un material menos peligroso o reducir la energía del sistema (por ejem
o que genere menos riesgo. (Definición Decreto 1072/2015)"

Control de ingeniería: "Instalar sistemas de ventilación, protección para las máquinas, enclavamient
(encerramiento) de un peligro o un proceso de trabajo, aislamiento de un proceso peligroso o del tra

Controles administrativos, señalización, advertencia: Instalación de alarmas, procedimientos de seg
al peligro, tales como la rotación de personal, cambios en la duración o tipo de la jornada de trabaj
trabajos seguros, controles de acceso a áreas de riesgo, permisos de trabajo, entre otros. (Definició

Equipos y elementos de protección personal: "Dar recomendaciones referentes al control de elemer
guantes. Etc. (Definición GTC - 45). Medidas basadas en el uso de dispositivos, accesorios y vestir
de trabajo. El empleador deberá suministrar elementos y equipos de protección personal (EPP) que
acuerdo con la identificación de peligros y evaluación y valoración de los riesgos. (Definición Decret

Al aplicar un control determinado se debe considerar los costos relativos, los beneficios de la reduc

3.12 Plan de acción

El plan de acción frente a los controles establecidos se incluirá en la matriz de registro y seguimient

3.13 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, investigació
- 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 demos

3.15 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 segu
de gestión.

3.16 Revisión de la valoración de riesgos

En forma periódica y cuando las condiciones cambien se debe realizar una revisión de la valoración

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

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 auditorí
- 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 in
publicarse en la intranet.

4 METODOLOGÍA PARA LA IDENTIFICACIÓN, EVALUACIÓN Y TRATAMIENTO DE RIESGOS D

Introducción

La presente metodología es propia de la SDM y se encuentra articulada con la Guía de administraci
un mayor alcance y robustez en la gestión de riesgos de soborno y de cara al mantenimiento del Sis

.

Objetivo

Establecer la metodología para la identificación, evaluación y tratamiento de los riesgos de soborno

4.1 Responsabilidades

Oficial de Cumplimiento Antisoborno

- Revisar periódicamente la matriz de riesgos de soborno.
- Realizar la evaluación de probabilidad e impacto de cada uno de los hechos de soborno identi
- Aprobar la matriz de riesgos de soborno.
- Socializar en el Comité Institucional de Gestión y Desempeño y con el Comité Técnico Antisob
- Informar al Comité Institucional de Gestión y Desempeño y al Comité Técnico Antisoborno sob
- Definir los controles antisoborno a aplicar a los riesgos con calificación de medio o alto que se
- Apoyar a las áreas que lo requieran en la definición de controles especiales de acuerdo a los r
- Aprobar el plan de tratamiento de riesgos.
- Aprobar el informe de seguimiento semestral a la matriz de riesgos de soborno.
- Socializar con el nivel directivo el informe de seguimiento semestral de la matriz de riesgos de

Comité Técnico Antisoborno

- Revisar la gestión realizada sobre los riesgos con calificación de medio y alto.
- Tomar decisiones frente a los controles que no sean efectivos.
- Garantizar la gestión de riesgos de soborno en la Entidad.
- Realizar seguimiento a los planes de tratamiento de los riesgos de soborno.

Profesional y/o contratista Subsecretaria de Gestión Corporativa

- Revisar la documentación relacionada con cada uno de los procesos para identificar actividad
- Identificar aquellos cargos que se ven expuestos a hechos de soborno.
- Revisar la evaluación de probabilidad e impacto de cada uno de los hechos de soborno identif
- Proponer el plan de tratamiento a los riesgos con calificación de medio y alto.
- Realizar las mesas de trabajo con los miembros del equipo técnico de calidad de las áreas pa
- Actualizar la matriz de riesgos de soborno cada vez que se requiera.
- Presentar al Oficial de Cumplimiento Antisoborno los resultados de la gestión de riesgos de so
- Apoyar a los contratistas (personas jurídicas y concesiones) en el levantamiento de riesgos de
- Velar por el cumplimiento de los controles adicionales definidos de acuerdo a los riesgos de so
- Realizar el seguimiento semestral a la matriz de riesgos de soborno, mediante la creación de u
- Realizar la verificación de las evidencias aportadas frente a la descripción de los controles y lo
- Elaborar el informe de seguimiento de la matriz de riesgos de soborno para la aprobación del

Miembros del Equipo Técnico de Calidad y/o líderes de proceso

- Revisar e identificar los posibles hechos de soborno determinados a sus áreas, sedes, proces
- Identificar los controles operativos existentes definidos para evitar la materialización de los ries
- Socializar con sus áreas la matriz de riesgos de soborno, garantizando la participación de los j
- Realizar el monitoreo periódico a la matriz de riesgos de soborno para garantizar la aplicación
- Realizar el reporte periódico y oportuno de las evidencias de cumplimiento de los controles op
- Informar al Oficial de Cumplimiento Antisoborno cada vez que se requiera ajustar la matriz de
- Socializar los informes de seguimiento de la matriz de riesgos de soborno con los dueños de l

4. 2 Lineamientos y/o políticas de operación

- La matriz de riesgos de soborno será revisada una vez al año con el fin de identificar nuevos h
- Se deberán contemplar todos los procesos de la Entidad para la identificación de riesgos de so
- Para los riesgos de soborno relacionados con terceros o contratistas que desempeñen funcior

- La gestión de riesgo estará alineada con las mejores prácticas definidas en la última versión d
- Es necesario que las personas y partes involucradas tanto internas como externas, estén info este proceso.
- Cuando el valor del riesgo residual es igual o mayor a 8 “riesgo MEDIO y ALTO”, se deberán e

a) Reducir la probabilidad de la Consecuencia del riesgo, minimizando la posibilidad de oc

b) Reducir el impacto de la Consecuencia (efecto del riesgo de soborno) sobre los objetivos antisob

- Cuando el nivel de riesgo es “BAJO”, es decir cuando su valor es menor o igual a 6, no es nec
- Los riesgos de soborno deben evaluarse por su probabilidad e impacto en una escala de 1 a 5

TABLA PARA LA CALIFICACION DE PROBAB	
VALOR	**DESCRIPCION**
1	El riesgo cuenta con controles fuertes y automatizados, adicional no hay sospecha de
2	El riesgo cuenta con controles fuertes pero manuales lo que puede generar incertidum
3	El riesgo cuenta con controles simples y manuales lo que puede generar incertidumbr
4	El riesgo cuenta con controles débiles lo que permite que la materialización de un ries
5	El riesgo no cuenta con controles y ha generado incertidumbre en los socios de negoc
TABLA PARA LA CALIFICACION DEL IMPACTO	
VALOR	DESCRIPCION
1	Afecta el cumplimiento de las metas en una actividad específica.
2	Afecta el cumplimiento de objetivos individuales y genera una queja o reclamo por par
3	Afecta los objetivos del proceso y genera algún tipo de llamado de atención en el área
4	Afecta fuertemente los objetivos estratégicos lo que ocasiona mayor presión de los en
5	Afecta la reputación de la Entidad y/o genera investigaciones en los funcionarios y cor

- **La Matriz de Configuración de la Severidad que refleja la ubicación de cada uno de los r**

Pr

- La mayor severidad que se puede dar de un riesgo de acuerdo a los rangos y tablas definidos
- Los controles son las políticas, procesos, dispositivos, prácticas u otras acciones que actúa antisoborno.
- El Equipo Técnico de Calidad deberá garantizar que los controles operativos existentes se Antisoborno.
- El Equipo Técnico de Calidad deberá definir quién es el responsable de ejecutar el control, la
- Como mínimo una vez al año se revisa y actualiza el mapa de riesgos de soborno de la entida
- Esta actualización es responsabilidad del Oficial de Cumplimiento Antisoborno quien, con el a
- El Oficial de Cumplimiento antisoborno y/o Equipo Antisoborno realizarán el monitoreo al ma 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

4.3 Desarrollo de la metodología

1. Revisar la documentación de cada uno de los procesos de la Entidad para identificar posibles
2. Documentar los posibles hechos de soborno y sus controles operativos existentes en el forma
3. Documentar quién es la persona responsable de ejecutar el control operativo existente, la peri
4. Validar que los posibles hechos de soborno identificados correspondan con las actividades pro
5. Aceptar que la información de la matriz es acorde con la realidad del proceso y que los hechos
6. Determinar el nivel de probabilidad (en una escala de 1 a 5 según el cuadro de criterios de pro fin de obtener el Riesgo Residual.
7. Definir en el formato plan de tratamiento del riesgo de soborno las actividades para los riesgos
8. Socializar la matriz de riesgos de soborno y los planes de tratamiento a cada una de las áreas

9. Realizar monitoreo y seguimiento a la ejecución de los controles operativos existentes.
10. Realizar seguimiento a la ejecución de las actividades del plan de tratamiento de riesgos de so
11. Evaluar la efectividad de las acciones propuestas en los planes de tratamiento de riesgos de s
12. Socializar ante la Alta Dirección los resultados del seguimiento a la matriz de riesgos de sobor

Materialización de riesgos de soborno

En el caso de la materialización de un hecho o riesgo de soborno se deberá realizar una revisión al

Si el control no se cumplió, se deberá realizar un análisis para identificar la causa raíz que origino la

5. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BAJO LA METODOLOGÍA DEL DEPARTAI

5.1 Metodología de Gestión de Riesgos de Seguridad de la Información

Integrando la metodología del Departamento Administrativo de la Función Pública y la guía de gest
Distrital de Movilidad gestione los riesgos de Seguridad de la información basado en los criterios de

Así mismo, tiene como objetivo proveer los lineamientos para que la entidad logre vincular la identifi

5.1.1 Identificación del riesgo de seguridad de la información

Para la identificación de los riesgos de seguridad de la Información, los procesos deben realizar ini
de activos de información. En este momento es importante establecer cuáles son los activos críticos

Una vez identificado el activo de información, clasificado, valorado y establecida su criticidad; los a
metodología de gestión de riesgos de seguridad de la información.

Para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de

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

Para cada riesgo, se debe asociar el activo o grupo de activos críticos y analizar las posibles amena

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes im

A continuación, se describen el conjunto de amenazas definidas por la entidad.

Identificación de Amenazas: Se plantea el siguiente listado de amenazas, que representan situacior

Tabla de Amenazas Comunes:

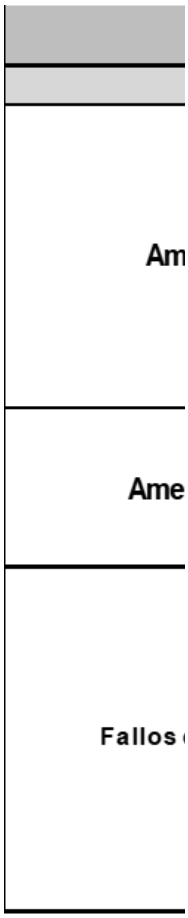


Tabla de vulnerabilidades comunes: La entidad define la identificación de vulnerabilidades en las sig

Nota: La sola presencia de una vulnerabilidad no causa daños por sí misma, dado que es necesario

TIPO D ACTIV
HARDW

TIPO D ACTIV
SOFTW

TIPO D
ACTIV

TIPO D ACTIV
RED

TIPO D ACTIV
PERSO

TIPO D
ACTIV

ORGANIZ

TIPO D
ACTIV

TIPO D ACTIV

Las consecuencias se describen como el impacto que puede generar en la entidad o en los procesc

A continuación, se puede observar un ejemplo de identificación del riesgo sobre un activo como la b

5.1.2 Análisis del Riesgo

En esta etapa se busca establecer la probabilidad de ocurrencia e impacto de la materialización de

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas a continuación

La determinación del impacto se entiende como la consecuencia económica y reputacional que se g

El líder del proceso como conocedor de su quehacer, define cuantas veces desarrolla la actividad, e

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el

A continuación, se muestra un ejemplo de identificación de zona de riesgo inherente (combinación e

Fuen
el Mi

5.1.3 Valoración de Controles

La entidad se alinea como mínimo a los controles establecidos en el Anexo A de la ISO/IEC 27001.

Claúsula o Domi
Controles Organizacionale
Controles de Personas

Fuente: Anexo A. ISO/IEC 27001

Una vez establecidos y valorados los riesgos inherentes se procede a la identificación y valoración d

El primer paso es hacer una identificación del control o controles que mitigaran el riesgo, este ejerc siguiendo la estructura sugerida a continuación:

- Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en ca
- Acción: Se determina mediante verbos que indican la acción que deben realizar como parte de
- Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del co

Luego, se realiza una clasificación y valoración de los controles teniendo en cuenta su tipología:

- Preventivos: Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurren
- Detectivos: Control accionado durante la ejecución del proceso. Estos controles detectan el rie
- Correctivos: Aquellos que permiten el restablecimiento de la actividad, después de ser detecta

Adicionalmente, los controles de acuerdo con la manera cómo se ejecuten se clasifican en:

- Automáticos: Aquellos que son ejecutados a través de un sistema o aplicativo.
- Manuales: Aquellos que son operados o ejecutados por una persona.

Finalmente, se evalúa el riesgo residual de acuerdo a los atributos de los controles, conforme a los

Tipo de control	
Preventivo	Aqu ocu
Detectivo	con det
Correctivo	Aqu det las
Automático	Aqu
Manual	Aqu

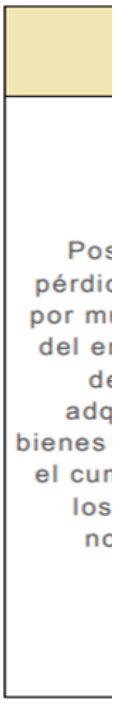
Atributos Informativos:

Característica		
Documentación	Documentado	Controles que está
	Sin documentar	Identifica aquellos
Frecuencia	Continua	El control se aplica
	Aleatoria	El control se aplica
Evidencia	Con Registro	El control deja un r
	Sin Registro	El control no deja r

A partir de estos criterios se establece la valoración del control y en tal sentido el desplazamiento er
impacto.

5.1.4 Valoración del riesgo residual

Con la información de la etapa anterior se procede a realizar el calculo del nivel de riesgo residual, c



Acorde a la información de cada control y su valoración en los atributos, se procede a realizar una c

- 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 probabilida

Valor de probabilidad antes de controles: 60%

Valor de atributos del control 1: 40%

60%*40% = 24%

Este último lo restamos al valor inicial de probabilidad

60% - 24% = 36%

Como para el ejemplo se tenían dos controles se toma el valor resultado del primero y de la misma

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

36%*30% = 10.8%

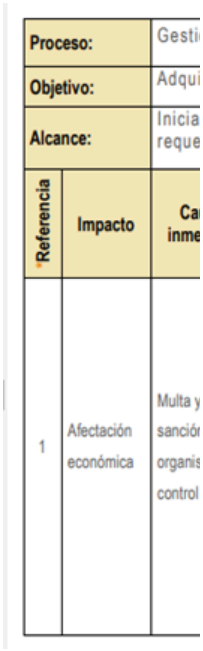
Nuevamente se resta del último valor de probabilidad que es 36%

36% - 10.8% = 25.2%

Teniendo como resultado final para probabilidad la nueva ubicación en el mapa de calor en un porce

Para los movimientos de impacto se realizan de la misma manera teniendo como referencia no la pr

En la siguiente tabla se encuentra un resumen del ejercicio de ejemplo hasta la valoración del riesg



Proceso:		Gesti
Objetivo:		Adqui
Alcance:		Inicia reque
Referencia	**Impacto**	**Ca inme**
1	Afectación económica	Multa y sanció organis control

5.1.5 Niveles de Aceptación del Riesgo

En esta etapa la entidad determina que para los riesgos que en su valoración residual se moderados, alto o extremos deberán ser objeto de la generación de un plan de tratamiento

5.1.6 Tratamiento del riesgo

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes rie
incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de éste y la relación co

El tratamiento o respuesta al riesgo, se enmarca en las siguientes categorías:

- **Aceptar el Riesgo**: No se adopta ninguna medida que afecte la probabilidad o el impacto del
- **Reducir- Mitigar el Riesgo**: Se adoptan medidas para reducir la probabilidad o el impacto del
- **Reducir- Compartir el Riesgo**: Se reduce la probabilidad o el impacto del riesgo transfiriendo
- **Evitar el Riesgo**: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o r

Se deben generar planes de acción para los riesgos, que en su valoración residual se encuentren e

En 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 activi
- **Aceptar**: No adoptando medidas que afecten la probabilidad y/o impacto.

Plan de Tratamiento de Riesgos de Seguridad de la Información

Corresponde a los líderes de los procesos establecer el plan de tratamiento de riesgos teniendo en

- Plan de Acción: Es el conjunto de actividades planteadas por el proceso para mitigar o reducir
- Responsable: Corresponde al cargo que se encargará de garantizar la ejecución del plan de a
- Fecha de Implementación: Es la fecha a partir de la cual se iniciará la implementación del plar
- Fecha de seguimiento: Es la fecha propuesta conjuntamente con el proceso de Gestión de Te
- Estado del Plan de Acción: Corresponde a la valoración emitida por el proceso de Gestión de
    - En curso
    - Cumplido
    - Modificado y
    - Cancelado

5.1.7 Seguimiento y Monitoreo del Plan de Acción

- Acciones que se realizaron para el cumplimiento del plan de acción: Corresponde a la descrip
- Evidencias: Descripción del conjunto de soportes que dan cuenta de la ejecución de la acción
- Observaciones: Corresponde a las observaciones y/o recomendaciones identificadas en el seg
- Análisis del Avance: Contiene la descripción realizada por la segunda línea de defensa frente a
- ¿Se materializó el Riesgo?: Campo dispuesto para indicar si el riesgo se materializó o no.
- ¿Se llevó a cabo el registro del incidente?: Campo dispuesto para indicar si se llevó a cabo el

La Oficina de Tecnologías de la Información y las Comunicaciones realizará seguimiento y monitore

- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de
- Verificar que los controles están diseñados e implementados de manera efectiva y operen com
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

6. METODOLOGÍA PARA LA IDENTIFICACIÓN, EVALUACIÓN Y TRATAMIENTO DE RIESGOS D

El objetivo de esta metodología es describir el paso a paso para identificar los riesgos potenciales a como las medidas que se han adoptado para el tratamiento de los riesgos, para asegurar la continu

Los objetivos específicos son:

- Identificar los riesgos de interrupción de los procesos transversales que podrían alterar la cont
- Realizar la identificación y clasificación de los controles existentes para la sede de la Calle 13
- 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 est

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 ocurrencia e impacto estimado.

Valoración de Riesgo:

Es un proceso general de identificación, análisis y evaluación de riesgos, materializados o potencial

Identificación Del Riesgo

En esta etapa del proceso, se busca determinar las fuentes de riesgo, los sucesos, causas y consec

El siguiente esquema, describe los niveles en los que se soporta la misión y operación de la ent interrupción, en la disponibilidad de los recursos que apoyan la operación misional, dado que su aus

Recursos claves

La identificación de riesgos de interrupción se realiza considerando la no disponibilidad de uno o va

Las técnicas utilizadas para realizar la identificación de los riesgos son entrevistas semiestructurada de las buenas prácticas, de procedimientos, tecnología e infraestructura, más aceptado y otros extra

- 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 Program
- ISO 22301:2019y
- Las buenas prácticas de continuidad de negocio y de recuperación ante desastres del DRI (Di

El proceso de identificación de riesgos de interrupción consiste en identificar las consecuencias, la entregadas por ellos a los cuestionarios.

La técnica de evaluación de estos cuestionarios, en la que siempre se evalúan respuestas cerrad frente a cada categoría de riesgo; la respuesta a cada pregunta puede ser positiva o negativa (la me

A continuación, un ejemplo de uno de los formularios para la identificación de riesgos relacionados c

Formulario: Identificación RA Recurso Humano (plan emergencia)

Tabla 1 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 c colaboradores no puedan actuar de tal manera que puedan salvaguardar su integridad física, ocasic

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 interrupc

Para cada proceso crítico se identifican y analizan las posibles amenazas y vulnerabilidades que po

Una amenaza tiene el potencial de causar una indisponibilidad de los recursos habilitadores (Infrae deliberadas, es recomendable identificar todos los orígenes de las amenazas accidentales como de

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 situa

A manera de ejemplo se citan las siguientes amenazas:

Tabla de Amenazas Comunes:

Tabla 2 Tabla de amenazas

TIPO	

Amenazas Físicas	Contaminación, Polvo, Corrosión.
	Niveles de temperatura o humedad por fuera de los rangos aceptal
	Incendio.
	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
Fallas técnicas	Falla del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
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 informátic
Cambio Climático	Modificación significativa y duradera de los patrones climáticos glo

Vulnerabilidades comunes: La entidad puede identificar vulnerabilidades (debilidades en las siguien

- 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 3 Tabla de vulnerabilidades

EJEMPLOS DE VULNERABILI
Mantenimiento
Ausencia de es
Susceptibilidad
Susceptibilidad
Almacenamien
Falta de cuidad
Copia no contr
Ausencia o insu
Defectos bien c

Disposición o re
Configuración i
Ausencia de co
Descarga y usc
Ausencia de co
Ausencia de pr
Punto único de
Ausencia de ide
Gestión inadec
Conexiones de
Ausencia del pe
Uso incorrecto
Falta de concie
Ausencia de m
Uso inadecuad
Ubicación en á
Red energética
Ausencia de pr

Ausencia de pr
Ausencia de pr
Ausencia de di
Ausencia de pr
Ausencia de re
Respuesta inac
Ausencia de ac
Ausencia de pr
Ausencia de pl

En la Imagen a continuación se puede observar un ejemplo de identificación del riesgo de interrupci

Tabla 4 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

Análisis Del Riesgo

La actividad de análisis de riesgo de interrupción consiste en establecer los criterios de riesgo asoc recursos claves, de acuerdo con los escenarios de interrupción establecidos para la entidad.

Esta etapa tiene como objetivo establecer los criterios de riesgo asociados a la probabilidad e impac
acuerdo con los escenarios de interrupción que se relacionan a continuación:

Tabla 5 Escenarios de Interrupción para Riesgos de Continuidad de Negocio

ESCENARIOS	

Escenarios de Impacto Global	Pandemias, Fenómenos meteorológicos, desac
Escenarios de Impacto Nacional, Regional o Local	Desastres naturales (como Terremotos, inundac
Escenarios de Impacto Particular	Ciberataques, inundaciones, incendios, desorde de los proveedores.

Se determina la probabilidad de ocurrencia que pueda tener el riesgo identificado y su impacto en c impacto determinará el riesgo inherente.

Tabla 6 Determinación de la probabilidad para riesgos de Continuidad de Negocio

Nivel	*Frecuer
1	Muy baj
2	Baja pro
3	Mediana
4	Significa
5	Casi cor

Determinar el impacto: para determinar el impacto se tendrán en cuenta los criterios de la Guía Para detención o afectación a otros procesos y el impacto operacional:

Tabla 7. Determinación del Impacto para Riesgo de Continuidad del Negocio

Riesgo Inherente:

Ilustración 2 Mapa de Calor de Riesgo Inherente para Riesgo de Continuidad de Negocio

Etapa de control:

Después de determinado el riesgo inherente, se deben establecer controles de tipo correctivos enca

- 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 e adecuada solución de infraestructura tecnológica, permite a la entidad restablecer las opera incidente o desastre que impacte a la Secretaria Distrital de Movilidad.

- La Estrategia de Continuidad de Negocio contempla alternativas de recuperación para respon
- Cada alternativa de recuperación propuesta está diseñada para cubrir, responder y recuperar
- Las alternativas de recuperación propuestas son viables y factibles de implementar para cada
- La presente Estrategia de Continuidad de Negocio se considera funcional al estar implementa

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

- Plan de Manejo de Crisis: establece los parámetros necesarios para tomar decisiones, gestion 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 d
- Planes de Recuperación ante Desastres: definen las acciones y tareas a seguir antes, durante
- Plan de Emergencias: Define el actuar ante situaciones de emergencias, con el fin salvaguard

c. Ejercicios de Continuidad: Consiste en un proceso para entrenar, evaluar, practicar y mejorar e desarrollada es capaz de proveer resultados de respuesta y recuperación ante una interrupció

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 demás elementos del SGCN.

Los controles en continuidad de negocio son de tipo correctivos, se deben evaluar los atributos para

- Para la calificación se tuvo en cuenta la implementación si era manual o automático, y Acción
- El 100% se dividió en estas 5 opciones, pero no de igual para todos, de acuerdo al DAFP prop
- 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%

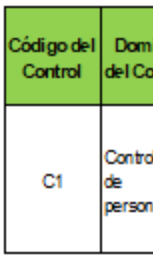
3. Contribuye directamente en la recuperación del proceso crítico afectado dentro de los tiempos ob

De acuerdo con lo anterior la calificación del control se calcula con la suma de los 2 atributos selecc

Características			
Atributos de Eficacia	Implementación	Automático	Son actividade realización.
		Manual	Controles que
	Acción Oportuna del Control	No contribuye directamente en la r	
		Contribuye parcialmente en la recu	
		Contribuye directamente en la recu	
*Atributos de Formalización	Documentación	Documentado	Controles que
		Sin Documentar	Identifica a los
	Evidencia	Con Registro	El control deja
		Sin Registro	El control no d

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

Tabla 8 Ejemplo de valoración de controles

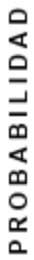


Código del Control	Dom del Co
C1	Contro de person

Riesgo Residual:

Como resultado del diseño y análisis de controles, se obtiene el riesgo residual que indicará el desp

Ilustración 3 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 generando una indisponibilidad de los servicios de tecnología y como consecuencia la interrupción cómputo alterno.

Tratamiento de los Riesgos:

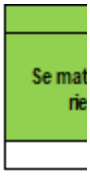
Después de establecido el riesgo residual, debe determinarse el tratamiento de los riesgos, el cual s

Las principales entradas para el mejoramiento de los riesgos de Continuidad de Negocio son los res

Por lo anterior, en este punto se analiza la respuesta a los incidentes de interrupción y se identifican

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

Tabla 9 Ejemplo de Tratamiento de riesgos de continuidad del negocio



Se mat rie

Etapa de monitoreo:

En esta etapa se lleva a cabo la revisión y actualización de los riesgos de Continuidad de Negocio c de continuidad, la implementación de nuevos proyectos al interior de la entidad, cambios en la pl riesgos o modificar la medición de probabilidad y/o impacto del riesgo a nivel inherente y/o residu tiempos establecidos.

Asimismo, la persona Oficial de Continuidad en ejercicio de su rol como segunda línea de defensa, de continuidad, ejercicios de continuidad, el programa de capacitación y sensibilización dirigido a to

Mediante la gestión de los incidentes de interrupción, se analizan aquellos riesgos que se hayan Dirección, del comportamiento de los indicadores de gestión del SGCCN, entre otros.

7. Metodología para la identificación, valoración y tratamiento de los riesgos para el Sistema

7.1 Identificación de riesgos

Análisis del contexto

La presente metodología sirve como referencia sobre los estándares relacionados con el riesgo herramientas básicas y las mejores prácticas generales para el diseño y posterior implementación p los canales de atención y las herramientas institucionales para controlas la materialización de riesgo

Factores de riesgo: Son los agentes generadores del riesgo de LA/FT. Para efectos del SARLAFT la

Producto/servicio:

Son las operaciones legalmente autorizadas que pueden adelantar las entidades vigiladas mediante

Cliente /usuario:

Cliente

Es toda persona natural o jurídica con la cual la entidad establece y mantiene una relación contractu

Son aquellas personas naturales o jurídicas a las que, sin ser clientes, la entidad les presta un servi

Contrapartes:

Las contrapartes: Son las personas naturales o jurídicas, nacionales o extranjeras, con las

cuales la entidad tiene algún tipo de relación legal o contractual en desarrollo de su objeto social p contractual, sugerimos extender los controles del riesgo de LA/FT a otras “contrapartes”

Canales:

Los canales: Uno de los factores de riesgo, que la literatura especializada en la gestión

de riesgo de LA/FT, considera debe ser objeto de administración son los “canales de distribución”. e

7.2 Redacción de causas, riesgo y consecuencias

Se busca poder identificar los riesgos de LA/ FT inherentes a la entidad en el desarrollo de su misio la administración de riesgos se busca identificar el qué, por qué y cómo pueden surgir los eventos d

C/

Causa: Se identifican los factores que causan de raíz la presentación del posible evento de riesgo, r

Evento: se relaciona como probabilidad de ocurrencia con el de contar con su identificación y prever

Consecuencia: Efectos sobre la presentación de la materialización del evento de riesgo.

7.3 Evaluación del riesgo

Evaluar los riesgos: es importante mencionar que los elementos consistentes en analizar y evaluar esto dependerá de la metodología que se seleccione y la rigurosidad del método. En todo caso, la e con el objetivo de identificar prioridades de administración de los riesgos, es decir, atender aquellos

Probabilidad:

Para la presente metodología se define los siguientes aspectos para el análisis de probabilidad:

CALCUL
M

Impacto

Los niveles de impactos están dados por el aumento de sus consecuencias y requieren de un conte

Riesgo inherente:

El riesgo inherente es el nivel de riesgo previo al establecimiento de controles, este nos permite defi

Su medición está dada por el análisis de la probabilidad y su impacto de manera matricial de la sigu

Este cuadro es llamado mapa de calor, y permite determinar en que nivel de riesgo inherente se en

7.4 Definición de controles

Esta etapa busca diseñar e implementar los controles y/o medidas que permitan controlar los ries naturaleza del riesgo de LA/FT, los controles que pueden y deben ser diseñados son de tipo prever con lo establecido en el marco normativo.

Control: Los controles deben relacionar quien lo ejecuta, la periodicidad de ejecución, de que trata e

Tipo de control: Teniendo en cuenta la naturaleza del riesgo, solo se deben definir controles de tipo

Tipo de implementación: Se define si el control se implementa de manera manual o automática.

Controles manuales: Son las acciones que realizan las personas responsables de un proceso o acti

Controles automáticos: Son procedimientos aplicados desde un computador, en un software de sop

Una vez se cuente con la definición de los controles estos deben ser evaluados dando respuesta a l

¿Ex
resp
asigr
ejecu
cc
califiqu
asi
0 si
asi

¿Las ac
se desa
contro
buscan
prevenir
causas
dar orig
ejemp
Valid
Compa

calif
previene
o 0 si no

Lo que nos permite conocer si el diseño del control es adecuado y saber a su vez cuando movimien

Una vez se realicen los movimientos en el mapa de calor podemos conocer cual es el nivel de riesg

7.5 Política de tratamiento

Aceptar: El nivel de riesgo residual es aceptado, se recomienda realizarlo únicamente cuando el ries

Mitigar: Realiza acciones complementarias para seguir mitigando la materialización del riesgo

Compartir: Comparte el riesgo y sus niveles con otro proceso de la entidad, así como definen respor

7.6 Monitoreo

Es responsabilidad de la entidad revisar el desempeño y funcionamientos del SARLAFT, periódicam
de mejora del sistema tomando acciones correctivas, preventivas y de eficiencia y eficacia de los co

8. Lineamientos generales de la guía

- Las actualizaciones a la presente guía se deben socializar en el Comité Institucional de Coord
- Cuando se requiera realizar un tema nuevo o actualizar algún capítulo, se debe solicitar por el
- Las actualizaciones realizadas a la presenta guía serán firmadas únicamente por los responsa

ELABORÓ DEL PROCESO	REVISÓ
Julio Roberto Fuentes Vidal Contratista 2025-10-28 17:19:45	Claudia Elena Parada Aponte Profesional Especializado(a) 222-19 2025-10-28 19:01:56