MANUAL PARA LA ADMINISTRACIÓN DEL RIESGO EN PROCESOS
SECRETARÍA DISTRITAL DE HACIENDA

Código: MN-9
Versión: 02
Vigente a partir de: 19/06/2024

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

La Secretaría Distrital de Hacienda – SDH, en cumplimiento de la normativa vigente, cuenta con la Política de Administración de Riesgo y Cumplimiento de la SDH alineada con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y el Modelo Integrado de Planeación y Gestión – MIPG.

Estos lineamientos son el fundamento para la construcción de este manual con el propósito de asegurar la adecuada administración de riesgos como habilitador para el cumplimiento de los objetivos estratégicos de la Secretaría Distrital de Hacienda, en adelante -SDH -.

La aplicabilidad de este manual le corresponde a los integrantes de cada una de las líneas de defensa y el rol que desempeñan en el marco de las mismas, las cuales se encuentran descritas en la Política de Administración de Riesgo y Cumplimiento.

Es importante mencionar que, la gestión de riesgos a nivel mundial ha venido cobrando relevancia en las últimas cinco décadas, es por ello que organizaciones abanderadas en el tema tales como el Comité de Supervisión Bancaria de Basilea el cual se constituyó en diciembre de 1974 como un foro de discusión para fomentar la mejora y convergencia de las prácticas y normas de supervisión bancaria, buscando perfeccionar las herramientas de fiscalización internacional, a través de acercamientos y estándares comunes.

En 1988 este organismo aprobó el Acuerdo de Capital de Basilea I, que introducía unas exigencias mínimas de recursos propios del 8% en función de los riesgos asumidos, principalmente de crédito.

Posteriormente, en junio de 2004 se crea el Acuerdo de Basilea II que corresponde a un estándar internacional de referencia para los reguladores bancarios, con el propósito de establecer la protección de las entidades frente a los riesgos financieros y operativos.

En respuesta a la crisis financiera mundial que se presentó entre 2007 y 2009, se creó el Acuerdo de Basilea III, este es un conjunto de medidas acordadas internacionalmente con el objetivo de reforzar la regulación, supervisión y gestión de riesgo en los bancos.

Otra de las organizaciones referencia para la gestión de riesgos es el Committee of Sponsoring Organizations of the Tradeway Commission – COSO (Establecido en Estados Unidos), compuesto por organismos privados, su objetivo es proporcionar un modelo común de orientación a las entidades sobre aspectos fundamentales como gestión ejecutiva y de gobierno, ética empresarial, control interno, gestión de riesgo empresarial, control de fraude y presentación de informes financieros. COSO ha venido evolucionando en términos de la gestión de riesgos, es así como en 1992 se publica el Internal Control – Integrated Framework (Informe COSO o COSO I) como marco integrado para ayudar a las empresas a evaluar y mejorar sus sistemas de control interno; posteriormente, en 2004 se publica el modelo COSO II o COSO ERM (Enterprise Risk Management) cuyo objetivo es permitir a las empresas mejorar su gestión de control interno mediante un proceso más completo de gestión de riesgos; en 2013 se publica el modelo COSO III, actualizado en el modelo COSO ERM 2017 que mejora el marco integrado para permitir una mayor cobertura de los riesgos a los que se enfrentan las organizaciones.

Basados en los pilares proporcionados los mencionados estamentos, los órganos de supervisión, regulación y control de los diferentes países han desdoblado estos

lineamientos a través de normatividad aplicable tanto a organizaciones del sector privado como a entidades gubernamentales en los diferentes sectores económicos.

Para el caso del sector público en Colombia, entidades tales como la agencia de contratación Colombia Compra Eficiente ha creado el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación, por su parte, el Departamento Administrativo de la Función Pública – DAFP- ha generado la Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas, lineamientos que la SDH ha tomado como referencia para desarrollar el sistema de administración de riesgo y cumplimiento, además de los documentos CONPES 4042 DE 2012 “Política Nacional Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva”, CONPES 01 de 2018 “Política Pública Distrital de Transparencia, Integridad y No Tolerancia con la Corrupción”, La ley 2195 de 2022 “Por medio de la cual se adoptan medidas en materia de transparencia y lucha contra la corrupción y se dictan otras disposiciones”, el estándar ISO 31001:2018, ISO 22301:2019 entre otros.

Es de señalar que el Sistema Integral de Administración de Riesgo - SIAR- de la SDH está compuesto por las etapas de identificación, medición, control y monitoreo, así como por los siguientes elementos:

- Comité de Riesgo.
- Política de Administración de Riesgo y Cumplimiento.
- Políticas de Seguridad de la Información y Tratamiento de Datos Personales.
- Macroproceso de Gestión Integral de Riesgo y Cumplimiento.
- Manual para la Administración del Riesgo en Procesos.
- Manual para la Construcción y Mantenimiento de la Continuidad de Negocio.
- Manual de Gestión de Crisis.
- Manual de Gestión de Riesgo Estratégico.
- Manual de Gestión de Seguridad de la Información.
- Procedimiento de Administración de Riesgos.
- Procedimiento de Gestión de Eventos de Riesgo.
- Procedimiento Monitoreo de Controles de Riesgos.
- Procedimiento Formulación, Ejecución y Evaluación del Plan del Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST.
- Procedimiento de Identificación de Aspectos y Valoración de Impactos Ambientales.
- Programa de sensibilización en materia de gestión de riesgos.
- Aplicativo para la administración del contenido de las matrices de riesgo en procesos y consulta en listas restrictivas y vinculantes.
- Matrices de Riesgos en proceso.
- Base de datos de reporte y gestión de eventos de riesgo.
- Reporte de monitoreo, ejecución y efectividad de controles.
- Reportes periódicos de la gestión de riesgos a instancias de administración y control interno.
- Reportes de la gestión de riesgos a demanda de los órganos de control externo.

Con respecto al programa de sensibilización, la estructura de la temática tiene una periodicidad anual y es objeto de revisión y actualización periódica, de acuerdo con las necesidades de la entidad, además, éste se armoniza e integra con el Plan Institucional de Capacitación y Desarrollo de Competencias incluidas la inducción y reinducción al cargo.

2. OBJETIVOS

2.1. Objetivo general

El Manual para la Administración del Riesgo en Procesos de la SDH tiene como objetivo desdoblar los lineamientos establecidos en la Política de Administración de Riesgo y Cumplimiento, establecer la metodología y procedimientos necesarios para asegurar una adecuada implementación del Sistema Integral de Administración de Riesgo en la entidad.

2.2. Objetivos específicos

- Promover el desarrollo de procesos internos basados en la gestión de riesgo, que permitan reducir la probabilidad y/o mitigar el impacto en caso de materialización de eventos de riesgo.
- Integrar las etapas de administración de riesgo de acuerdo con los roles asignados a cada línea de defensa.
- Gestionar la administración de riesgos por proceso a través del software vigente en la entidad.
- Socializar a los funcionarios, contratistas y particulares que ejerzan funciones públicas en la entidad, la metodología de administración de riesgos por procesos.

3. ALCANCE

La gestión de riesgos por procesos inicia con la identificación del contexto interno y externo de la organización y de cada proceso, continua con las actividades que permiten desarrollar las etapas de identificación, medición de riesgo inherente, establecimiento y evaluación de controles, determinación del nivel de riesgo residual, diseño de planes de tratamiento y mejora continua que incorporando el seguimiento y monitoreo permanente de los riesgos y controles respectivamente.

Es importante señalar que no existe como tal un fin de la gestión de riesgos por procesos, toda vez que corresponde a un círculo virtuoso compuesto por las diferentes fases de la gestión de riesgo.

4. APETITO DE RIESGO

Corresponde al nivel de riesgo establecido por la Alta Dirección, que la entidad está dispuesta a asumir en el desarrollo de sus procesos, para dar cumplimiento a sus metas y objetivos. Para la SDH el apetito de riesgo se estableció de la siguiente manera:

- Cero tolerancias a los riesgos de incumplimiento legal o normativo y los relacionados con actividades delictivas que puedan presentarse por omisión, negligencia, y/o intención en las tipologías de riesgo de corrupción, legal y LAFTFPADM (Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva). Sin embargo, para éstos últimos, debido a que el modelo de referencia para la diagramación en el mapa de calor del SARLAFT es el generado por el Departamento Administrativo de la Función Pública – DAFP en términos de valoración del riesgo de corrupción, podrán existir riesgos de LA/FT/FPADM residuales en la zona de Nivel Extremo, Alto y Medio, los cuales deberán tener un seguimiento por parte del Oficial de Cumplimiento con el propósito de no descuidar

su evolución.

- Para todas las demás tipologías de riesgo por procesos la SDH declara como no tolerables aquellos riesgos ubicados en el Nivel Extremo y Nivel Alto.
- Los riesgos ubicados en Nivel Moderado son tolerables y aquellos en Nivel Bajo se consideran aceptables.
- Para todos los riesgos de tipo legal y fiscal solo son aceptables los riesgos o eventos de riesgo que se encuentren en un nivel de riesgo residual Bajo.

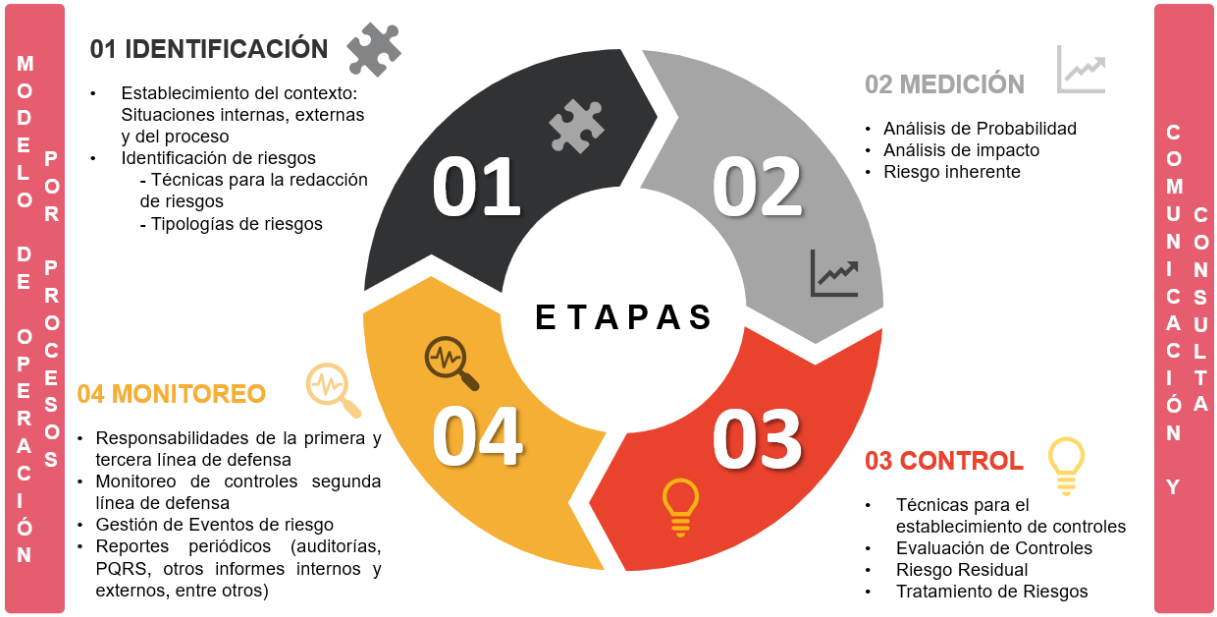
5. TIPOLOGÍAS DE RIESGOS

El Manual para la Administración del Riesgo en Procesos de la SDH contempla la gestión de los riesgos que se agrupan en las siguientes tipologías:

- Riesgo Operacional
- Riesgo de Corrupción
- Riesgo Fiscal
- Seguridad Digital, Seguridad de la información
- Continuidad del Negocio
- Riesgos de Seguridad y Salud en el Trabajo
- Riesgos Ambientales
- Riesgo de LA/FT/FPADM - Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

La Administración del Riesgo se fundamenta en los lineamientos establecidos en la Política de Administración de Riesgo y Cumplimiento de la SDH, en virtud de la cual deben surtirse las siguientes etapas para todas las tipologías de riesgo:

Ilustración 1. Etapas de la Administración del Riesgo en la SDH



5.1. RIESGO OPERACIONAL

Se entiende por riesgo operacional la posibilidad de que la entidad incurra en pérdidas por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano, así como por la ocurrencia de acontecimientos externos asociados a éstos, que afecten el desarrollo de las operaciones, la continuidad del negocio, la disponibilidad, integridad y confidencialidad de la información, el medio ambiente, la salud y/o la integridad de los servidores públicos. Incluye el riesgo legal.

5.1.1. Etapa de Identificación:

La etapa de identificación se desarrolla a través de las siguientes fases:

a. **Análisis de contexto:** Corresponde al ambiente interno y externo del proceso y de la entidad que puede afectar la ejecución normal de los procesos, dificultando la consecución de sus objetivos; este análisis incluye situaciones externas tales como: el ambiente socio-cultural, político, legal, reglamentario, financiero, tecnológico, económico, ambiental, las tendencias que tienen impacto en los objetivos de la organización; y las relaciones con las partes interesadas externas.

   Respecto del análisis de situaciones internas, se tienen en cuenta el: gobierno, la estructura organizacional, los manuales de funciones, las políticas, los objetivos y estrategias, las capacidades(entendidas en términos de recursos y conocimientos por ejemplo, capital, tiempo, infraestructura física, personas, procesos, sistemas y tecnologías), las partes interesadas internas, la cultura de la organización, infraestructura tecnológica, flujos de información y procesos de toma de decisiones, normas, directrices y modelo de gestión de la entidad, relaciones contractuales.

   La SDH ha definido que el análisis del contexto lo realizará a partir de una matriz DOFA.

b. **Puntos de Riesgo:** Se analizan detalladamente las actividades del proceso para determinar cuáles son críticas y pueden generar la materialización de un riesgo, se cuenta con evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operacional.

c. **Identificación de las áreas de impacto:** Corresponden a los criterios de valoración que serán tenidos en cuenta al momento de evaluar el impacto que podría tener el riesgo en caso de materializarse.

d. **Identificación de factores de riesgo:** Se entiende por factores de riesgo las fuentes generadoras de riesgo que están asociadas directamente a las causas, estas pueden ser: procesos, talento humano, tecnología, infraestructura y evento externo.

e. **Descripción del riesgo:** Para la descripción del riesgo se utilizan las preguntas ¿Qué? ¿Cómo? ¿Por qué?, las cuales permiten determinar cuál es el impacto, la causa principal y las secundarias.

5.1.2. Etapa de Medición:

A través de la etapa de medición se determina la probabilidad de ocurrencia que pueda tener el riesgo identificado y su impacto en caso de materializarse, esta medición se realiza

utilizando los criterios establecidos en una tabla de probabilidad y otra de impacto de cinco (5) niveles cada una, el cruce entre la probabilidad y el impacto determinará el riesgo inherente (riesgo en su estado puro).

a. **Determinar la probabilidad:** Para determinar la probabilidad se tienen n en cuenta criterios cualitativos y cuantitativos, basados en la posibilidad de ocurrencia o el registro del número de eventos entre un (1) año y tres (3) años.

Tabla 1. Determinación de Probabilidad para Riesgo en procesos

NIVEL		PROBABILIDAD CUALITATIVA	PROBABILIDAD POR EVENTO	PROBABILIDAD PORCENTUAL
5	Casi Seguro	Se espera que evento ocurra en la mayoría de las circunstancias.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último mes	Se espera la ocurrencia del evento en más del 20% de los casos
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último semestre	El evento ocurrirá entre el 15% y el 20% de los casos
3	Posible	El evento podría ocurrir en varios casos.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último año	El evento ocurrirá entre el 10% y el 15% de los casos
2	Improbable	El evento puede ocurrir en algún momento.	Existe evidencia de que el evento se ha presentado por lo menos una vez en los últimos 2 años	El evento ocurrirá entre el 5% y el 10% de los casos
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (Poco comunes o anormales).	Existe evidencia de que el evento se ha presentado por lo menos una vez en los últimos 3 años	El evento puede ocurrir en menos del 5% de los casos

b. Determinar el impacto: Para determinar el impacto se tendrán en cuenta los siguientes criterios:

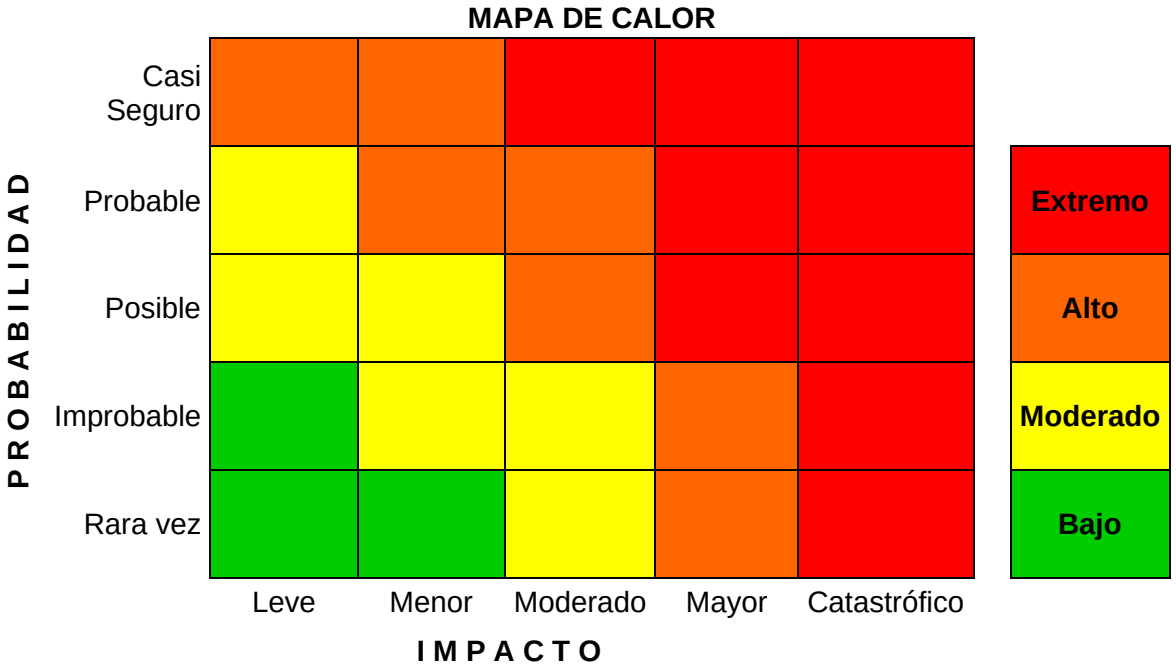
Tabla 2. Determinación de Impacto para Riesgo en Procesos

NIVEL		ECONÓMICO	REPUTACIONAL	LEGAL	OPERACIÓN	CONTAGIO	CORRUPCIÓN
5	Catastrófico	Afectación mayor a 500 SMLMV	Afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido en medios de comunicación a nivel local y/o país	Intervención (Plan de saneamiento) de la entidad por parte de un órgano de control u otro regulador	Podría generarse un impacto alto para la SDH al detenerse el proceso por 8 horas o menos. Si el proceso se detiene puede afectar o detener toda la cadena de valor. Reprocesos o carga operativa adicional para otras entidades.	Causado por un representante del Gobierno o Administración del Distrito Capital	Responder afirmativamente de DOCE a DIECINUEVE (12 a 19) preguntas
4	Mayor	Afectación entre 100 a 500 SMLMV	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Entidades distritales), respecto al cumplimiento de sus objetivos	Multas o sanciones administrativas para la entidad por parte de entes de inspección, vigilancia y/o control	Podría generarse un impacto alto para la SDH al detenerse el proceso por un rango de tiempo entre 1 y 3 días. Si el proceso se detiene, puede detener más de un proceso misional. Se generan reprocesos o carga operativa adicional para otros procesos o dependencias.	Causado por un funcionario de alto nivel de la SDH	Responder afirmativamente de SEIS a ONCE (6 a 11) preguntas
3	Moderado	Afectación entre 50 a 100 SMLMV	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Contribuyentes), respecto al cumplimiento de sus objetivos	Demandas a la entidad por parte de tercero ante jueces de lo contencioso administrativo	Podría generarse un impacto alto para la SDH al detenerse el proceso por un rango de tiempo entre 3 y 5 días. Si el proceso se detiene puede afectar un proceso	Causado por un funcionario o contratistas de la SDH	Responder afirmativamente de UNO a CINCO (1 a 5) pregunta(s)

NIVEL		ECONÓMICO	REPUTACIONAL	LEGAL	OPERACIÓN	CONTAGIO	CORRUPCIÓN
					misional, o puede generar reprocesos en este.		
2	Menor	Afectación entre 10 a 50 SMLMV	Afecta la imagen de la entidad internamente (entre sus funcionarios y Directivos), y el tema es abordado en Comités Directivos y otras instancias internas	Investigaciones, sanciones, inhabilidades, entre otras, de tipo disciplinario, fiscal y/o penal en contra de alguno(s) de los funcionarios de la entidad	Podría generarse un impacto alto para la SDH al detenerse el proceso por un rango de tiempo entre 5 y 10 días. Si el proceso se detiene afecta o detiene a un proceso no misional.	Causado por un usuario (contribuyentes)	N/A
1	Leve	Afectación menor a 10 SMLMV	No hay una afectación relevante a la imagen de la entidad	Hallazgos administrativos, observaciones o recomendaciones producto de auditorías	Podría generarse un impacto alto para la SDH al detenerse el proceso por un periodo mayor a 15 días. Si el proceso se detiene, no hay afectación sobre otros procesos. No se generan reprocesos.	Causado por un tercero interesado	N/A

c. **Riesgo Inherente:** La combinación entre la probabilidad y el impacto determina el nivel de riesgo inherente en cualquiera de las cuatro zonas establecidas (bajo, moderado, alto y extremo):

Ilustración 2. Mapa de Calor de Riesgo Inherente para Riesgo en procesos



5.1.3. Etapa de Control:

En esta etapa se establecen medidas para mitigar el riesgo inherente identificado y realizar tratamiento a los riesgos residuales que superen el nivel de tolerancia establecido.

Después de determinado el riesgo inherente, se deben e identificar controles encaminados a reducir la probabilidad de ocurrencia y/o el impacto del riesgo identificado. Para describirlos se deben tener en cuenta los siguientes elementos:

- El responsable de ejecución corresponde al cargo de la persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso.

- Establecer la acción, es decir, el cómo se va a ejecutar el control, iniciando con un verbo en infinitivo, como, por ejemplo, revisar, validar, verificar, corroborar, conciliar, comparar, cotejar.

- Definir el complemento, es decir, los requisitos necesarios y tareas adicionales para ejecutar el control.

Para surtir esta etapa se requiere definir una serie de atributos que permitirán establecer si el diseño del control es o no, adecuado, los atributos son:

a. **Responsable:** El control debe indicar en su descripción el responsable asignado para su ejecución.

b. **Oportuno:** Para establecer la oportunidad, es necesario identificar si la periodicidad del control es consistente, es decir, que coincide con el registro de la frecuencia de ejecución de la actividad en la cual podría generarse el riesgo.

c. **Tipo de control:** Para clasificar el control debe identificarse en qué momento dentro de la ejecución del proceso se activa, lo cual permitirá determinar su tipología, es decir, que puede ser preventivo, detectivo o correctivo.

d. **Naturaleza del control:** Corresponde a la forma de ejecución del control, permite establecer si éste depende de una persona (manual), de un sistema (automático), o combinado.

e. **Documentado:** Para evaluar esta variable, debe determinarse si el control se encuentra documentado. Se considera documentado, cuando existe en algún documento del Sistema de Gestión, alguna norma (ley, decreto, resolución interna o externa, circular, memorando) u otro tipo de documento tal como política, acta de comité, etc.

f. **Evidencia:** Es todo aquello que permita probar la ejecución del control y es esta variable la que permite conocer si el control cuenta o no con evidencia de su ejecución.

g. **Descripción de la evidencia:** El detalle de la evidencia específica del control, corresponde a la forma en la que va a demostrarse que se ha ejecutado, por ejemplo, con un formato diligenciado, una comunicación, un correo electrónico, una marca en un aplicativo, archivos en diferentes formatos, entre otros.

h. **Frecuencia:** Corresponde a la periodicidad de ejecución del control, que puede ser diaria, semanal, quincenal, mensual, bimestral, trimestral, cuatrimestral, semestral, anual, continua (funciona de manera permanente, ininterrumpida, sin embargo, su activación se da por una condición como por ejemplo, los controles de seguridad física o lógica) y esporádica (en este caso el control se ejecuta por demanda, como por ejemplo, los controles correctivos que comúnmente se ejecutan después de ocurrida la falla).

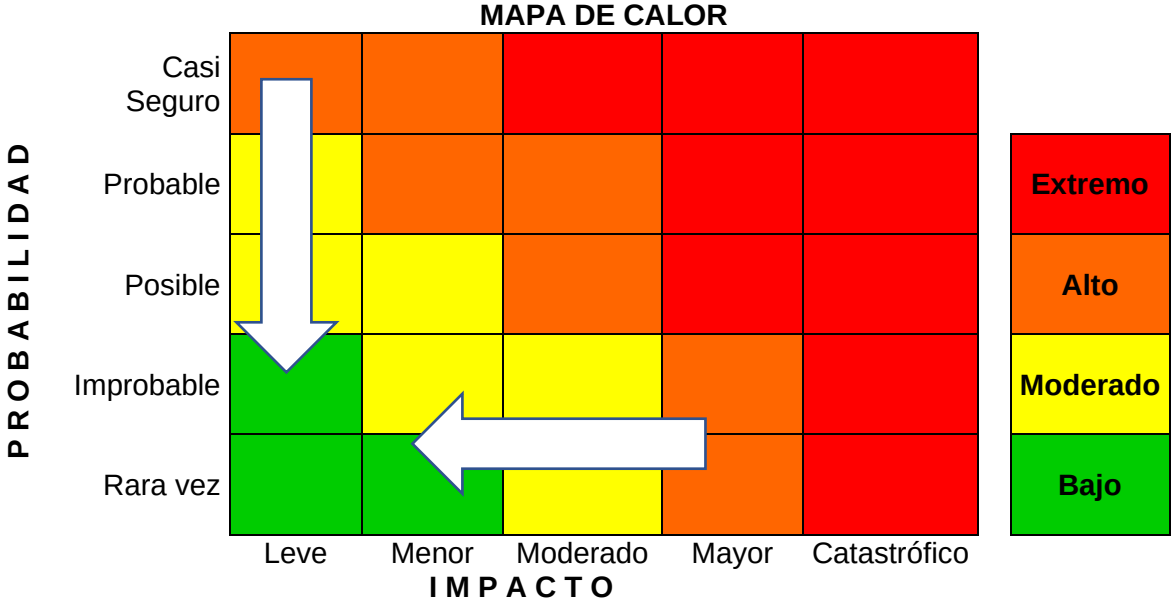
i. **El control disminuye:** cuando el control es preventivo o detectivo, disminuye la probabilidad y cuando éste es correctivo, disminuye el impacto.

j. **Riesgo residual:** Como resultado del diseño y análisis de controles, se obtiene el riesgo residual que indicará el desplazamiento del riesgo a un nivel inferior de acuerdo con la efectividad del control de la siguiente manera:

Tabla 3.Desplazamiento del Riesgo Residual Según la Efectividad del Control para la mitigación del riesgo en procesos

EVALUACIÓN DEL CONJUNTO DE CONTROLES			DESPLAZAMIENTOS
Promedio del conjunto de controles	Fuerte	81-100	2
	Moderado	61-80	1
	Débil	0-60	0

Ilustración 3. Mapa de Calor de Riesgo Residual para Riesgo en Procesos



Los controles preventivos y detectivos desplazan la probabilidad.
Los controles correctivos desplazan el impacto.

k. Tratamiento de los riesgos: Después de establecido el riesgo residual, debe determinarse el tipo de tratamiento para los riesgos, que no es otra cosa que la toma de decisiones frente a los resultados obtenidos. El tratamiento debe realizarse de acuerdo con lo establecido en la Política de Administración de Riesgo y Cumplimiento.

Las opciones de tratamiento para los riesgos en proceso se presentan a continuación:

- **Mitigar:** Se implementan acciones que disminuyen el riesgo.

- **Transferir o compartir:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.

  Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia (aseguradoras o contratistas). Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

- **Evitar o eliminar:** se eliminan aquellas actividades dentro del proceso que pueden dar origen a un riesgo.

- **Aceptar:** Se asume el riesgo conociendo las consecuencias que traería su materialización.

  De llegar a presentarse casos excepcionales en los cuales se identifiquen riesgos que ante la capacidad de mitigación actual de la Entidad no sea posible ubicarlos en los niveles de riesgo tolerables, éstos deberán ser aceptados de manera expresa por parte de los responsables del proceso y con el aval de la Alta Dirección y el comité de riesgos.

5.1.4. Etapa de Monitoreo:

a. **Monitoreo de controles:** Esta etapa esta alineada con la Dimensión 7 “Control Interno” del Modelo Integrado de Planeación y Gestión – MIPG - y la Política de Administración de Riesgo y Cumplimiento de la SDH para determinar responsables y acciones de acuerdo con las líneas de defensa.

Como segunda línea de defensa, anualmente la OACR verifica la efectividad de los controles establecidos en las matrices para la mitigación de los riesgos de procesos, con el propósito de asegurar que estos sean apropiados y funcionen correctamente. Este ejercicio se realiza mediante la recolección de evidencias, las cuales permiten evaluar y calificar cada uno de los controles. Resultado de lo anterior se generan conclusiones y recomendaciones generales, adicionalmente, en caso de ser necesario se realizan actualizaciones en las matrices de riesgo en proceso. Esta actividad se encuentra documentada en el procedimiento de Monitoreo de controles de riesgo en procesos 123-P-02.

b. **Gestión de eventos de riesgo:** También, la OACR lidera la gestión de los eventos de riesgo que sean reportados por parte de las áreas. Éstos son sujetos de investigación para establecer si supone una materialización de un riesgo, si este hace parte de la matriz de riesgo en proceso y tiene identificadas las causas que lo generan y el(los) control(es) que lo mitiga(n). Para el caso de las situaciones relacionadas con la materialización de riesgos de de Continuidad del Negocio y Seguridad de la Información, el término que se utiliza es “gestión de incidentes”, para esta última tipología de riesgo, el detalle de la gestión se complementa con el numeral 21 “Lineamientos para la gestión de incidentes de seguridad de la información del Manual de gestión de Seguridad de la Información MN-5.

c. En caso de ser necesario, se establece un Plan de Tratamiento (dependiendo del tipo de acción, se solicitará el acompañamiento de un representante de la OAP en su rol de oficina asesora, en caso de ser necesario) por parte de las dependencias, con el propósito de mitigar la ocurrencia del evento en el futuro y la actualización de la matriz de riesgo en procesos. Esta actividad se encuentra documentada en el procedimiento de Gestión de eventos de riesgo 123-P-03.

d. Las dependencias como primera línea de defensa deben solicitar el acompañamiento de la OAP para proponer las respectivas acciones frente al

tratamiento de un riesgo materializado y presentarlas a la OACR para su VoBo previo a la realización de los trámites necesarios para su radicación.

5.2. RIESGO DE CORRUPCIÓN

Se entiende por Riesgo de Corrupción la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

La SDH ha adoptado completamente la metodología de administración de riesgos de corrupción determinada por el Departamento Administrativo de la Función Pública - DAFP en la Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas.

5.2.1. Etapa de Identificación:

En la etapa de identificación es necesario para la descripción del riesgo tener en cuenta todos sus componentes:

Ilustración 4. Componentes de la Etapa de Identificación para Riesgo de Corrupción

Para facilitar el desarrollo de las actividades de esta etapa, se puede utilizar la matriz de definición que permite visualizar los componentes de manera individual para validar que los cuatro (4) estén presentes dentro de la descripción:

Tabla 4. Matriz de Definición del Riesgo de Corrupción

MATRIZ DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado

5.2.2. Etapa de Medición:

En la etapa de medición se establece la probabilidad de ocurrencia que pueda tener el riesgo identificado y su impacto en caso de materializarse, esta medición se realiza a través de una tabla de probabilidad de cinco (5) niveles y una de impacto que determinará a partir de un cuestionario de consecuencias el nivel que tenga el riesgo identificado (moderado, mayor, catastrófico).

a. **Valoración de probabilidad:** Deben tenerse en cuenta los criterios de factibilidad y/o frecuencia, el primero si no se cuenta con datos y solamente se hace un análisis de contexto para evaluar la posibilidad de ocurrencia, el segundo cuando se cuenta con datos de materialización del evento en un periodo determinado de tiempo:

Tabla 5. Valoración de Probabilidad para Riesgo de Corrupción

	CRITERIO DE FACTIBILIDAD	CRITERIO DE FRECUENCIA
Rara Vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
Improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
Posible	El evento podrá ocurrir en algún momento.	Al menos una vez en los últimos 2 años
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año
Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

b. **Valoración de impacto:** para calificar el impacto en los riesgos de corrupción, existe un cuestionario en la Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas del DAFP, en el cual según el número de preguntas afirmativas se establece el nivel de impacto:

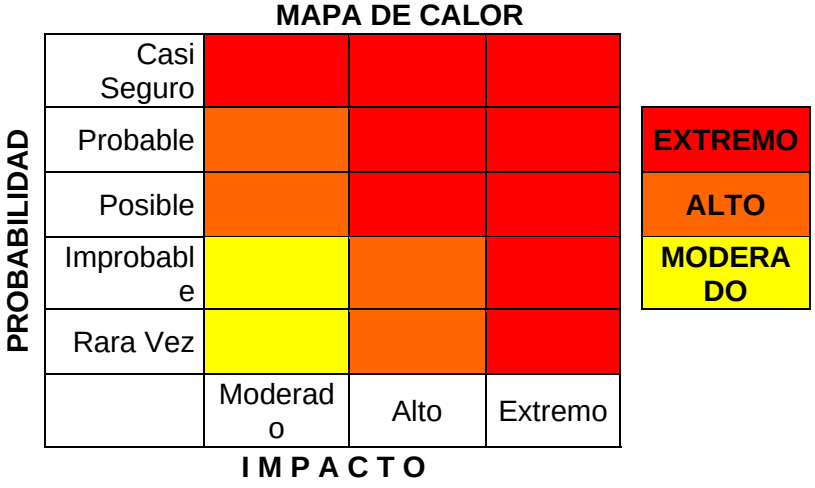
Tabla 6. Valoración de Impacto para Riesgo de Corrupción

FORMATO PARA DETERMINAR EL IMPACTO			
Nº	**Pregunta** ¿Si el riesgo de corrupción se materializa podría…?	Respuesta	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Genera pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		

FORMATO PARA DETERMINAR EL IMPACTO			
Nº	**Pregunta** ¿Si el riesgo de corrupción se materializa podría…?	Respuesta	
		SI	NO
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
CALIFICACIÓN	Total preguntas afirmativas		
	Total preguntas negativas		
	Nivel		
	MODERADO: Genera medianas consecuencias sobre la entidad. UNA a CINCO pregunta (s) genera un impacto moderado		
	ALTO: Genera altas consecuencias sobre la entidad. SEIS a ONCE preguntas genera un impacto mayor		
	EXTREMO: Genera consecuencias desastrosas para la entidad. DOCE a DIECINUEVE preguntas genera un impacto catastrófico		

c. **Riesgo Inherente:** El cruce entre la probabilidad y el impacto determina el nivel de riesgo inherente; para el caso de los riesgos de corrupción, de acuerdo con los lineamientos contenidos en la Guía para la administración del riesgo y el diseño de controles emitida por el Departamento Administrativo de la Función Pública, se tienen solamente tres (3) niveles: moderado, alto y extremo, no existen riesgos de corrupción que no generen ningún impacto, por eso los niveles insignificante y menor no son tenidos en cuenta:

Ilustración 5. Mapa de Calor Riesgo Inherente para Riesgo de Corrupción



5.2.3. Etapa de Control:

Los controles de riesgo de corrupción se evalúan en términos de diseño y ejecución.

Para evaluar el diseño de los controles asociados a la mitigación de los riesgos de corrupción se tienen en cuenta seis (6) determinantes:

a. **Responsable:** persona encargada de ejecutar la actividad establecida como control.

b. **Periodicidad:** establecer el momento y/o tiempo en que se ejecuta el control (diario, mensual, trimestral, anual).

c. **Propósito:** ¿Qué busca evitar o mitigar la actividad del control?

d. **¿Cómo se realiza?:** ¿Qué insumos se requieren para la ejecución del control?

e. **Observaciones o desviaciones:** medidas a tomar por parte del responsable del proceso cuando hay fallas en el control.

f. **Evidencia:** son todos los soportes con los que se cuenta para demostrar que el control se ejecutó de la forma en que se describe en la matriz de riesgo.

Tabla 7.Variables para la evaluación del diseño de los Controles asociados a la mitigación del Riesgo de Corrupción

CRITERIO	VARIABLE
Responsable	ASIGNADO
	NO ASIGNADO
Oportunidad	OPORTUNO
	NO OPORTUNO
Tipo	PREVENTIVO
	DETECTIVO
	CORRECTIVO
Naturaleza	AUTOMATICO
	COMBINADO
	MANUAL
Documentado	DOCUMENTADO
	NO DOCUMENTADO
Evidencia	CON EVIDENCIA
	SIN EVIDENCIA

Para la ejecución del control se evalúan tres niveles (débil, moderado, fuerte):

Tabla 8. Criterios determinantes para evaluar la ejecución de los controles asociados a la mitigación de los Riesgos de Corrupción

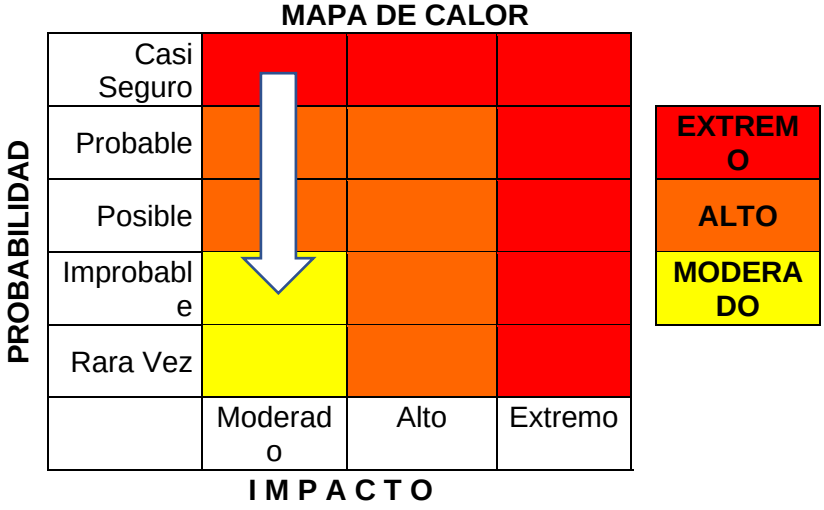
RESULTADO-PESO DE LA EJECUCIÓN DEL CONTROL	RANGO DE CALIFICACIÓN DE LA EJECUCIÓN
El control se ejecuta de manera consistente por parte del responsable.	FUERTE
El control se ejecuta algunas veces por parte del responsable.	MODERADO
El control no se ejecuta por parte del responsable.	DÉBIL

g. **Riesgo Residual:** El desplazamiento en la matriz colorimétrica para los riesgos de corrupción aplica únicamente para el criterio de probabilidad, el de impacto siempre se mantendrá igual al inicialmente identificado y dependerá de la combinación de los siguientes criterios.

Tabla 9. Criterios de Desplazamiento en la escala de probabilidad para los Riesgos de Corrupción

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	No. DE COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD
Fuerte	Directamente	2
Fuerte	Directamente	2
Fuerte	Directamente	2
Fuerte	No disminuye	0
Moderado	Directamente	1
Moderado	Directamente	1
Moderado	Directamente	1
Moderado	No disminuye	0

Ilustración 6. Matriz colorimétrica Riesgo de Corrupción



h. **Tratamiento de los Riesgos:** Después de establecido el riesgo residual, debe determinarse el tratamiento de los riesgos de corrupción, que no es otra cosa que la toma de decisiones (reducir, evitar y compartir) frente a los resultados obtenidos:

- **Reducir:** Se implementan acciones que disminuyen el riesgo.
- **Compartir:** Se terceriza el proceso o traslada el riesgo a través de seguros o pólizas, con lo cual la responsabilidad económica recae en el tercero más no la responsabilidad reputacional.

- **Evitar:** se eliminan aquellas actividades dentro del proceso que pueden dar origen a un riesgo de corrupción.

5.2.4. Etapa de Monitoreo:

Esta etapa esta alineada con la Dimensión 7 “Control Interno” de MIPG y la Política de Administración de Riesgo y Cumplimiento de la SDH para determinar responsables y acciones de acuerdo con las líneas de defensa.

Como segunda línea de defensa, con periodicidad anual la OACR verifica la efectividad de los controles establecidos en las matrices para la mitigación de los riesgos en procesos, con el propósito de asegurar que estos sean apropiados y funcionen correctamente. Este ejercicio se realiza a partir de la solicitud y posterior recepción de las evidencias de ejecución de los controles, las cuales se evalúan con base en una estructura de nueve (9) aspectos que permiten calificar cada uno de los controles . Resultado de lo anterior, se generan conclusiones y recomendaciones generales, en caso de ser necesario, se recomienda a los responsables de proceso realizar actualizaciones en las matrices de riesgo. Esta actividad se encuentra documentada en el procedimiento monitoreo de controles.

También, la OACR lidera la gestión de los eventos de riesgo que sean reportados por parte de las áreas a la dependencia. Éstos son sujetos de investigación para establecer si supone una materialización de un riesgo, si este se encuentra establecido en la matriz, sus causas, y el control aplicado. En caso de ser necesario, se establece un plan de tratamiento (dependiendo del tipo éste se solicitará mediante la OAP) con las áreas con el fin de mitigar la ocurrencia del evento en el futuro y su actualización de la matriz de riesgos. Esta actividad se encuentra documentada en el procedimiento Gestión de eventos de riesgo.

5.3. RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos de la categoría Seguridad de la Información dentro de los procesos se identifican y valoran siguiendo el mismo ciclo de gestión de riesgos que ha sido mencionado en los numerales anteriores para Riesgo Operacional. Para la calificación de su impacto se incluyen los criterios de disponibilidad, integridad y confidencialidad de la información, los cuales se gestionan con base en la metodología establecida en el Manual de gestión de seguridad de la información MN-5 (numeral 7.1 Metodología para la gestión de riesgos) y son insumo para la matriz de riesgo de Seguridad de la Información.

Los riesgos de la categoría Seguridad de la Información dentro de los procesos se identifican y valoran siguiendo el mismo ciclo de gestión de riesgos usado para el Riesgo Operacional (5.1), asimismo, para la calificación de su impacto se consideran los criterios de disponibilidad, integridad y confidencialidad de la información. Para que sean incluidos en la matriz por proceso, se consideran los que impactan la información de mayor criticidad para establecer el tratamiento necesario.

Los riesgos de Seguridad de la Información son identificados en cada proceso y su gestión se complementa con la metodología descrita en el Manual de gestión de seguridad de la información MN-5 (numeral 7.1 Metodología para la gestión de riesgos) dado que en ella se indica cómo gestionar los riesgos transversales de la entidad.

5.4. RIESGO DE CONTINUIDAD DEL NEGOCIO

Las etapas de la gestión de riesgos de continuidad de negocio son las mismas que se utilizan para el riesgo operacional. En razón a ello, los riesgos de continuidad de negocio se incluyen dentro de la matriz de riesgo operacional (por proceso) de la SDH; los riesgos cuya consecuencia implica la interrupción del proceso pueden presentarse por factores de riesgo tales como:

- Evento externo
- Infraestructura
- Talento humano (ausentismo o indisponibilidad del talento humano)
- Tecnología
- Registros vitales

5.4.1. Etapa de Identificación:

La etapa de identificación de los riesgos de Continuidad de Negocio se desarrolla a partir de la siguiente fase:

a. **Análisis de Riesgos de Interrupción (RA):** En esta fase se identifican los riesgos potenciales a los que está expuesta la Entidad y que podrían causar una alteración, interrupción o pérdida de las operaciones en los procesos de la entidad.

   Se identifican como parte del análisis de impacto al negocio que se desarrolla en cada proceso.

   Los riesgos de Continuidad de Negocio son riesgos operacionales cuya consecuencia es la interrupción del proceso, por la materialización de una amenaza, originada por la indisponibilidad total o parcial de los recursos mínimos requeridos o recursos habilitadores (tecnología, proveedores críticos, información, funcionarios) de la entidad.

5.4.2. Etapa de Medición:

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

Tabla 10. Escenarios de Interrupción para Riesgo de Continuidad de Negocio

ESCENARIOS	DESCRIPCIÓN DEL ESCENARIO
Escenario de Falla de Servicios Tecnológicos	Fallas en la infraestructura del centro de cómputo principal, Bases de Datos y aplicaciones de la Entidad; fallas en redes y comunicaciones, ataque cibernético.
Escenario de Indisponibilidad de los colaboradores	Eventos de tipo natural, social y/o antrópico (terremoto y/o sismo, orden público, sabotaje, vandalismo, terrorismo, fugas de gas y/o

	incendio etc.), Intoxicación masiva, epidemia, pandemia.
Escenarios de Impacto Global que afecten la infraestructura	Pandemias, fenómenos meteorológicos, desaceleración económica global, cambios climáticos, conflictos políticos globales.
Escenarios de Impacto Nacional, Regional o Local que afecte la infraestructura	Desastres naturales en el país o en la ciudad de Bogotá como terremotos, inundaciones, huracanes, sismos, orden público, epidemias, endemias, cambios climáticos, sabotaje, vandalismo, terrorismo, manifestaciones, bloqueos).
Escenarios de Impacto Particular que afecte la infraestructura	Situaciones que afecten únicamente a la Secretaría Distrital de Hacienda tales como problemas de orden público, sabotaje, vandalismo, terrorismo, manifestaciones, bloqueos, fugas de gas y/o incendio, inundación, suspensión prolongada de servicios públicos, fallas en los equipos críticos etc.
Escenario de indisponibilidad de proveedores críticos	Contratación a corto plazo de servicios que se requieren en mediano y largo plazo. Ausencia o fallas en el plan de contingencia y continuidad de los proveedores.
Escenario de Indisponibilidad de los Registros Vitales	No acceso, pérdida o destrucción de los registros vitales.

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

a. **Determinar la probabilidad:** Para determinar la probabilidad se tendrá en cuenta el número de eventos de interrupción en el periodo de tres (3) años:

Tabla 11. Determinación de la Probabilidad para Riesgo de Continuidad de Negocio

NIVEL		PROBABILIDAD CUALITATIVA	PROBABILIDAD POR EVENTO	PROBABILIDAD PORCENTUAL
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último mes	Se espera la ocurrencia del evento en más del 20% de los casos
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último semestre	El evento ocurrirá entre el 15% y el 20% de los casos
3	Posible	El evento podría ocurrir en varios casos.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último año	El evento ocurrirá entre el 10% y el 15% de los casos

NIVEL		PROBABILIDAD CUALITATIVA	PROBABILIDAD POR EVENTO	PROBABILIDAD PORCENTUAL
2	Improbable	El evento puede ocurrir en algún momento.	Existe evidencia de que el evento se ha presentado por lo menos una vez en los últimos 2 años	El evento ocurrirá entre el 5% y el 10% de los casos
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (Poco comunes o anormales).	Existe evidencia de que el evento se ha presentado por lo menos una vez en los últimos 3 años	El evento puede ocurrir en menos del 5% de los casos

b. Determinar el impacto: para determinar el impacto se tendrán en cuenta los criterios de la Guía Para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP (reputacional y económico) y adicionalmente las afectaciones en la información, la operación y de tipo legal:

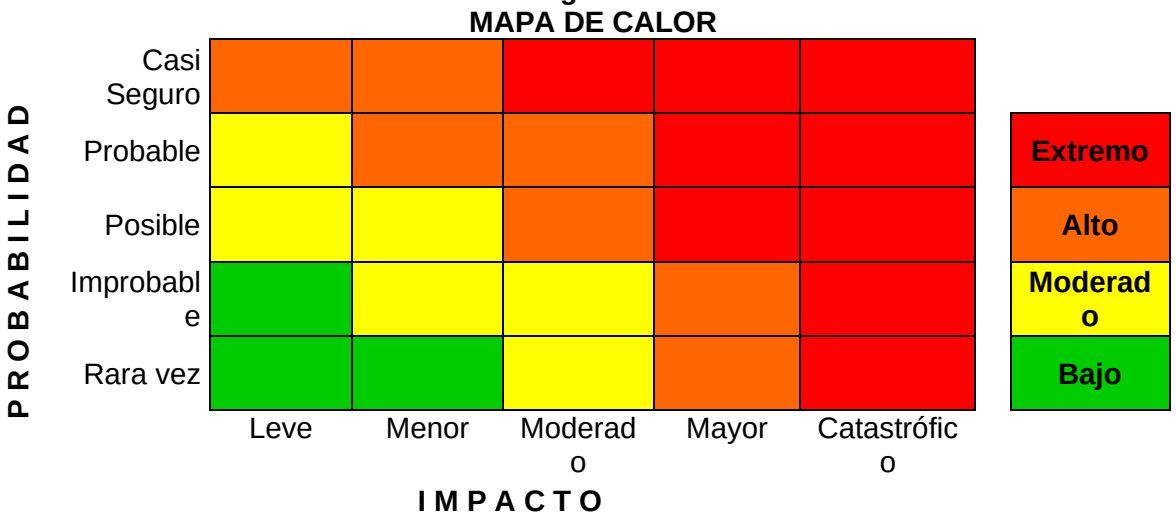
Tabla 12. Determinación del Impacto para Riesgo de Continuidad del Negocio

NIVEL		ECONÓMICO	REPUTACIONAL	LEGAL	OPERACIÓN
5	Catastrófico	Afectación mayor a 500 SMLMV	Afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido en medios de comunicación a nivel local y/o país	Intervención (Plan de saneamiento) de la entidad por parte de un órgano de control u otro regulador	Podría generarse un impacto alto para la SDH al detenerse el proceso por 8 horas o menos. Si el proceso se detiene puede afectar o detener toda la cadena de valor. Reprocesos o carga operativa adicional para otras entidades.
4	Mayor	Afectación entre 100 a 500 SMLMV	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Entidades distritales), respecto al cumplimiento de sus objetivos	Multas o sanciones administrativas para la entidad por parte de entes de inspección, vigilancia y/o control	Podría generarse un impacto alto para la SDH al detenerse el proceso por un rango de tiempo entre 3 y 1 día. Si el proceso se detiene, puede detener más de un proceso misional. Se generan reprocesos o carga operativa adicional para otros procesos o dependencias.
3	Moderado	Afectación entre 50 a 100 SMLMV	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Contribuyentes), respecto al cumplimiento de sus objetivos	Demandas a la entidad por parte de tercero ante jueces de lo contencioso administrativo.	Podría generarse un impacto alto para la SDH al detenerse el proceso por un rango de tiempo entre 5 y 3 días. Si el proceso se detiene puede afectar un proceso misional, o

NIVEL		ECONÓMICO	REPUTACIONAL	LEGAL	OPERACIÓN
				Silencio Administrativo Positivo.	puede generar reprocesos en este.
2	Menor	Afectación entre 10 a 50 SMLMV	Afecta la imagen de la entidad internamente (entre sus funcionarios y Directivos), y el tema es abordado en Comités Directivos y otras instancias internas	Investigaciones, sanciones, inhabilidades, entre otras, de tipo disciplinario, fiscal y/o penal en contra de alguno(s) de los funcionarios de la entidad	Podría generarse un impacto alto para la SDH al detenerse el proceso por un rango de tiempo entre 5 y 10 días. Si el proceso se detiene afecta o detiene a un proceso no misional.
1	Leve	Afectación menor a 10 SMLMV	No hay una afectación relevante a la imagen de la entidad	Hallazgos administrativos, observaciones o recomendaciones producto de auditorías. No existe ningún impacto legal.	Podría generarse un impacto alto para la SDH al detenerse el proceso por más de 15 días. Si el proceso se detiene, no hay afectación sobre otros procesos. No se generan reprocesos.

c. Riesgo inherente: La combinación entre la probabilidad y el impacto determina el nivel de riesgo inherente en cuatro zonas (bajo, moderado, alto y extremo):

Ilustración 7. Mapa de Calor de Riesgo Inherente para Riesgo de Continuidad del Negocio



5.4.3. Etapa de Control:

Después de determinado el riesgo inherente, deben establecerse controles encaminados a reducir la probabilidad y/o el impacto del riesgo identificado. Para surtir esta esta etapa se necesita:

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

Actualmente, la entidad cuenta con los siguientes controles para abordar los riesgos de continuidad del negocio:

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

   - La Estrategia de Continuidad de Negocio contempla alternativas de recuperación para responder a un incidente de interrupción que afecte la operación de la entidad.
   - Cada alternativa de recuperación propuesta está diseñada para cubrir, responder y recuperar el proceso en su momento más crítico.
   - Las alternativas de recuperación propuestas son viables y factibles de implementar para cada uno de los procesos críticos de la entidad.

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

   - **Plan de Manejo de Crisis**: La entidad cuenta con el MN-11 Manual de Gestión de Crisis, el cual establece los parámetros necesarios para tomar decisiones, gestionar, coordinar, evaluar, analizar una crisis, recuperar y mantener las operaciones a un nivel predeterminado en caso de ocurrir una interrupción y un procedimiento básico de comunicaciones a seguir en caso de enfrentar una situación de crisis.

   - **Planes de Continuidad por Proceso Crítico**: Describen la guía de acción para administrar posibles incidentes de interrupción que enfrente Secretaría Distrital de Hacienda, permitiendo la continuidad de la operación de acuerdo con los objetivos de recuperación definidos en el Análisis de Impacto, Análisis de Riesgo y la Estrategia Global de Continuidad de Negocio.

     Los Planes de Continuidad de Negocio se encuentran disponibles en el aplicativo MIGEMA, y hacen parte de la documentación de cada uno de los procesos críticos.

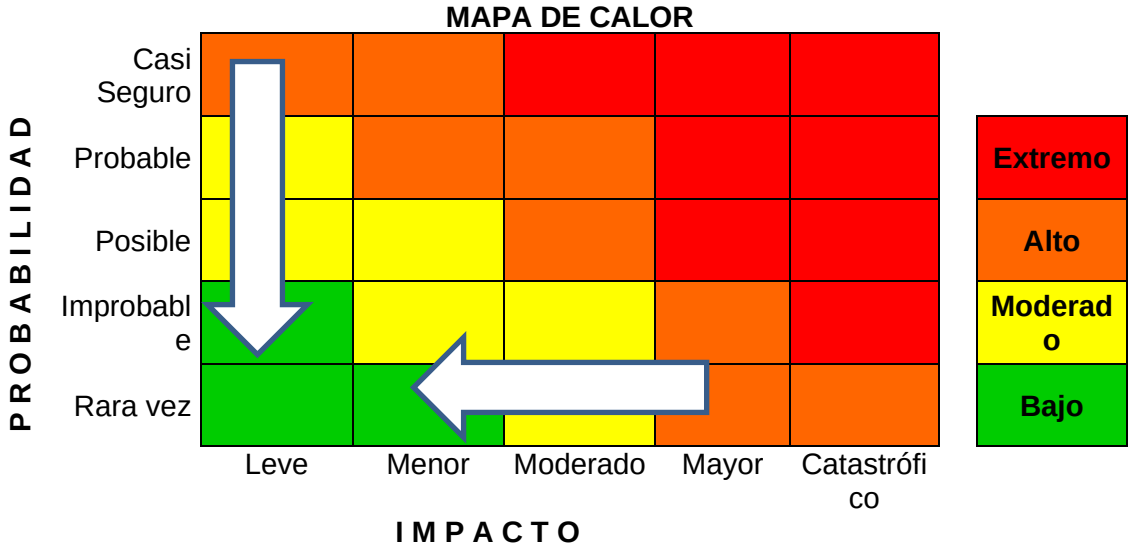
   - **Plan de Emergencias**: Define el actuar ante situaciones de emergencias, con el propósito de salvaguardar la integridad física de las personas y de las instalaciones físicas.

c. **Ejercicios o pruebas de Continuidad:** La entidad cuenta con un programa de ejercicios como herramienta de validación de los Planes de Continuidad de Negocio**,** con el propósito de entrenar, evaluar, practicar y mejorar el desempeño de la entidad.

d. **Capacitación y sensibilización:** El Sistema de Gestión de Crisis y Continuidad del Negocio - SGCCN, se socializa y sensibiliza a los funcionarios de la entidad a través de las semanas del riesgo desarrolladas anualmente en la entidad.

e. **Riesgo Residual:** Como resultado del diseño y análisis de controles, se obtiene el riesgo residual que indicará el desplazamiento del riesgo a un nivel inferior de acuerdo con la efectividad del control tal como se muestra a continuación:

Ilustración 8. Mapa de Calor de Riesgo Residual para Riesgo de Continuidad del Negocio



f. **Tratamiento de los Riesgos:** Después de establecido el riesgo residual, debe determinarse el tratamiento de los riesgos, que no es otra cosa que la toma de decisiones frente a los resultados obtenidos. El tratamiento debe realizarse de acuerdo con lo establecido en la política de administración de riesgos y cumplimiento.

- **Mitigar:** Se implementan acciones que disminuyen el riesgo.

- **Transferir o compartir:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.

  Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia (aseguradoras o contratistas). Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

- **Evitar o eliminar:** se eliminan aquellas actividades dentro del proceso que pueden dar origen a un riesgo.

- **Aceptar:** Se asume el riesgo conociendo las consecuencias que traería su materialización.

  De llegar a presentarse casos excepcionales en los cuales se identifiquen riesgos que ante la capacidad de mitigación actual de la Entidad no sea posible ubicarlos en los niveles de riesgo tolerables, éstos deberán ser aceptados de manera expresa por parte de los responsables del proceso y con el aval de la Alta Dirección y el Comité de Riesgo.

5.4.4. Etapa de Monitoreo:

a. **Monitoreo de controles:** Esta etapa debe estar alineada con la Dimensión 7 de MIPG y la Política de Administración de Riesgo y Cumplimiento de la SDH para determinar responsables y acciones de acuerdo con las líneas de defensa.

   Como segunda línea de defensa, anualmente la OACR verifica la efectividad de los controles establecidos en las matrices para la mitigación de los riesgos de los procesos, con el fin de asegurar que estos sean apropiados y funcionen correctamente. Este ejercicio se realiza mediante la recolección de evidencias, las cuales permiten evaluar y calificar cada uno de los controles. Resultado de lo anterior se generan conclusiones y recomendaciones generales, además, en caso de ser necesario se pueden realizar actualizaciones en las matrices de riesgo. Esta actividad se encuentra documentada en el procedimiento .

b. **Gestión de eventos de riesgo:** También, la OACR lidera la gestión de los eventos de riesgo que sean reportados por parte de las áreas. Éstos son sujetos de investigación para establecer si supone una materialización de un riesgo, si este se encuentra establecido en la matriz, sus causas, y el control aplicado. En caso de ser necesario, se establece un plan de tratamiento (dependiendo del tipo éste se solicitará mediante la OAP de ser necesario) con las áreas con el fin de mitigar la ocurrencia del evento en el futuro y su actualización de la matriz de riesgos. Esta actividad se encuentra documentada en el procedimiento de monitoreo de controles.

5.5. RIESGO DE SEGURIDAD Y SALUD EN EL TRABAJO

La gestión de riesgos de seguridad y salud en el trabajo en la SDH está a cargo de la Dirección de Gestión Corporativa.

La gestión de esta tipología de riesgo permite establecer el nivel de exposición al peligro en el que se encuentra un funcionario en ejercicio de sus labores y permite a la entidad brindar las garantías necesarias para trabajar en un entorno seguro.

La metodología para la identificación y valoración de riesgos y peligros de seguridad y salud en el trabajo está fundamentada en la Guía Para La Identificación de los Peligros y la Valoración de los Riesgos de Seguridad y Salud Ocupacional - Guía Técnica Colombiana - GTC 45, el procedimiento 112-P.03 Formulación, Ejecución y evaluación del Plan del Sistema de Gestión de Seguridad y Salud en el Trabajo Sg-Sst, instructivo 112-I.03

Ejecución del Subprograma de Higiene y seguridad Industrial y el instructivo 112-I.04 Ejecución del Subprograma de Medicina Preventiva y del Trabajo.

Las etapas de identificación, medición, control, monitoreo y seguimiento de los riesgos de seguridad y salud en el trabajo se desarrollan así:

5.5.1. Etapa de Identificación:

La identificación de los riesgos de seguridad y salud en el trabajo se lleva a cabo bajo las siguientes actividades:

a. **Definición y recolección de información:** consiste en conocer el entorno de la organización con el fin de identificar los peligros ocupacionales a los cuales están expuestos los funcionarios, como las condiciones de trabajo y de salud en todas las sedes de la entidad para darle prioridad a las condiciones de seguridad, higiene y salud para su control. Para ello se utilizan fuentes de información tales como: Matriz de Peligros o Panorama de factores de riesgo, estadísticas de morbilidad y accidentalidad laboral, informe de seguimiento y avance a los casos diagnosticados de enfermedades de origen común o laboral, evaluación del SG-SST por la ARL de las actividades realizadas anualmente, entre otros.

b. **Clasificación de procesos, actividades y tareas:** se establece una lista de las actividades que las áreas desarrollan dentro de la entidad para determinar el nivel de riesgo de cada una (ergonómicos, psicosociales, biológicos).

c. **Identificación de peligros:** La identificación de peligro se fundamenta en los riesgos ocupacionales, que se clasifican en 7 grupos y están definidos en la GTC-45, para los cuales, se analiza desde el entorno, la manipulación o ejercicio de la labor del funcionario que se está evaluando. Los grupos de clasificación de los riesgos ocupacionales de acuerdo con la guía son:

   - Biológico
   - Físico
   - Químico
   - Psicosocial
   - Biomecánicos
   - Condiciones de seguridad
   - Fenómenos naturales

   Para identificar los peligros, se deben tener en cuenta preguntas como:

   - ¿Existe una situación que pueda generar daño?
   - ¿Quién (o qué) puede sufrir daño?
   - ¿Cómo puede ocurrir el daño?
   - ¿Cuándo puede ocurrir el daño?

   Posteriormente para establecer posibles efectos de los peligros y niveles de daño, en el corto plazo (accidente de trabajo) y en el largo plazo (salud, enfermedades), se debe tener en cuenta otras preguntas como:

- ¿Cómo pueden ser afectados el trabajador o la parte interesada expuesta?
- ¿Cuál es el daño que le(s) puede ocurrir?

d. Identificación de controles existentes: se identifican los controles existentes para los peligros identificados y se clasifican en fuente, medio e individuo.

5.5.2. Etapa de Medición:

Para la medición y/o valoración de los riesgos de seguridad y salud en el trabajo se desarrollan las siguientes actividades:

a. Se determina los criterios de aceptabilidad del riesgo teniendo en cuenta aspectos como el cumplimiento de los requisitos legales, la Política Subsistema De Gestión De Seguridad Y Salud En El Trabajo - SG-SST, los objetivos y metas de la entidad, entre otros.

b. Se determina el nivel de riesgo mediante la multiplicación del nivel de probabilidad de ocurrencia del riesgo por el nivel de consecuencia.
A su vez, el nivel de probabilidad se determina a través de la multiplicación entre el nivel de deficiencia por el nivel de exposición.
Los criterios y asignación de valores, determinación del nivel de riesgo y su significado se encuentran en la GTC-45.

c. Se decide qué categorías de riesgos son aceptables y cuáles no lo son, estableciendo criterios de aceptabilidad de acuerdo con la normativa vigente y la consulta a las partes interesadas.

d. La información se consolida y se priorizan las condiciones de Seguridad y Salud en el Trabajo identificadas.

5.5.3. Etapa de Control:

Los controles son todas las medidas de intervención que se toman para reducir los peligros. Para establecerlos se desarrollan las siguientes actividades:

a. Se elabora la propuesta del Plan del Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST de acuerdo con el resultado de la valoración de riesgos, se decide si se requiere crear, mantener o mejorar los controles y el plazo para ejecutar las acciones.
Para la priorización y establecimiento de controles se deben tener en cuenta al menos los siguientes criterios: número de trabajadores expuestos, peor consecuencia y existencia de un requisito legal establecido.
Para establecer controles nuevos o mejorar los existentes se deben priorizar de acuerdo con el principio de eliminación de peligros y reducción de riesgos, es decir, reducción de la probabilidad de ocurrencia o la severidad potencial de la lesión o daño.
También se debe tener en cuenta los siguientes criterios:

- **Eliminación:** Consiste en eliminar la fuente del riesgo.
- **Sustitución:** Consiste en sustituir la fuente de peligro por un material menos peligroso o reducir la energía del sistema que cumpla la misma función minimizando el peligro.

- **Controles de ingeniería:** Consiste en el diseño de controles en sitio que reduzcan el nivel de riesgo.
- **Controles administrativos:** Hace referencia al establecimiento de controles a partir de procedimientos, manuales, instructivos ejemplos, señalizaciones, toma de temperatura, control de acceso.
- **Equipos y elementos de protección personal:** Consiste en la entrega de elementos de protección a los servidores requeridos para la ejecución de sus labores con el propósito de reducir su exposición al riesgo.

b. **Se revisa y da Vo. Bo. a la propuesta del plan del Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST**, se presenta al Comité de Gestión y desempeño de MIPG para sus comentarios y observaciones.

5.5.4. Etapa de Monitoreo y seguimiento:

Para desarrollar el monitoreo y seguimiento se debe determinar que actividades requieren contratación. El Plan del Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST se deberá implementar y ejecutar teniendo en cuenta los instructivos asociados al procedimiento 112-P.03.

Los resultados de la ejecución se evalúan para determinar el cumplimiento de las actividades planeadas, así como comparar los resultados obtenidos con los criterios definidos en la normatividad vigente. Además, la evaluación comprende los indicadores propios del SG-SST y las acciones de mejora para continuamente preservar, mantener y mejorar la salud individual y colectiva de los funcionarios de la entidad y el medio ambiente laboral y prevenir los accidentes de trabajo y las enfermedades laborales.

De acuerdo con lo anterior, se elabora un informe anual con la información consolidada de la ejecución, lo cual permite una revisión global que sirve para generar los ajustes al plan de la siguiente vigencia y finalmente se presenta al Subdirector de Talento Humano para su aprobación.

5.6. RIESGO AMBIENTAL

Esta tipología de riesgo está a cargo de la Dirección de Gestión Corporativa y se contempla en el proceso CPR-117Gestión Ambiental, con el procedimiento asociado 117-P-03 “Identificación de Aspectos y valoración de Impactos Ambientales”, en el cual se identifican y registran los aspectos para controlar y valorar los impactos ambientales que se generan a causa del desarrollo de los procesos de gestión de la Secretaría Distrital de Hacienda.

La metodología utilizada para la identificación y valoración de esta tipología de riesgos está fundamentada en el Instructivo de Diligenciamiento de la Matriz de Identificación de aspectos y valoración de impactos ambientales que establece la Secretaría Distrital de Ambiente y se resume en el procedimiento mencionado anteriormente.

Las etapas de identificación, medición, control, monitoreo y seguimiento de los riesgos ambientales se desarrollan así:

5.6.1. Etapa de Identificación de aspectos e impactos ambientales:

Para esta etapa, la Subdirección Administrativa y Financiera debe designar un funcionario como apoyo del PIGA, quien deberá identificar los aspectos ambientales a través de las siguientes actividades:

a. Revisar los procesos internos de la SDH y analizar las actividades y productos (bienes y servicios) que interactúan con el ambiente en diferentes escenarios, mediante mesas de trabajo con las áreas que lo requieran.
b. Definir la regularidad y/o frecuencia de ocurrencia de las actividades y/o productos bajo los siguientes criterios:

- Normal: Recurrente o frecuente.
- Anormal: Poco frecuente.
- Emergencia: De forma impredecible.

c. Asociar las actividades identificadas con los aspectos ambientales definidos por la Secretaría Distrital de Ambiente y consolidarlos en el formato “Planificación” de la Secretaría Distrital de Ambiente.

d. De acuerdo con los aspectos ambientales asociados en el punto anterior, se identifican los impactos ambientales según lo definido por la Secretaría Distrital de Ambiente y se relacionan en el mismo formato “Planificación”.

5.6.2. Etapa de Medición y/o valoración de los impactos ambientales:

La medición del impacto ambiental consiste en una interpretación cuantitativa, a través de unas escalas de valor fijas, de los atributos del impacto ambiental y el cumplimiento normativo de acuerdo con el aspecto ambiental. Esta etapa la desarrolla el funcionario como apoyo del PIGA con las siguientes actividades:

a. Se identifica y selecciona el recurso, elemento o componente ambiental (aire, agua, suelo, flora y fauna), que interactúa con el aspecto ambiental y que puede afectar positiva o negativamente el impacto ambiental. Se registra en el formato “Planificación”.

b. Se define el tipo de impacto (signo) de acuerdo con dos criterios, y se registra en el formato “Planificación”:

- Positivo (+) que significa una mejora en la calidad ambiental del recurso, la entidad y/o el entorno.
- Negativo (-) que hace referencia al deterioro de la calidad ambiental del recurso, la entidad y/o el entorno.

c. Se valora y se identifica la importancia de los impactos ambientales definidos a través de la tabla de valoración del impacto ambiental establecida por la Secretaría Distrital de Ambiente, donde se multiplica la escala de valor (1, 5 o 10) asignado a cada criterio de valoración (alcance, probabilidad, duración, recuperabilidad, cantidad y normatividad), y se determinará su rango de importancia de acuerdo al resultado (alta, moderada, baja), y su significancia (significativo o no significativo).

5.6.3. Etapa de Control:

Una vez obtenida la calificación de los impactos ambientales, se deben identificar los controles o acciones que permitan mantenerlos en un nivel permitido, disminuirlos o evitarlos:

a. Si el impacto ambiental es significativo con rango de importancia moderado, se debe definir un control operacional como manuales, bitácora y actividades de mantenimiento.
b. Si el impacto ambiental es significativo con rango de importancia alta se deben establecer mecanismos de mejora, control y seguimiento como procedimientos, actividades de registro y medición, auditorías, entre otros.
c. Si el impacto ambiental tiene un rango de importancia baja y se evidencia el cumplimiento de la normativa se puede establecer el seguimiento al desempeño ambiental como control operacional.

5.6.4. Etapa de Monitoreo y seguimiento:

La información ingresada en el formato “Planificación” es revisada por el funcionario de apoyo al PIGA y lo remite al Gestor Ambiental para su aprobación, si requiere ajustes lo devuelve a la SDH para su corrección y posterior envío formal a la Secretaría Distrital de Ambiente a través del aplicativo dispuesto para ello.

Los controles definidos deben ser implementados por los funcionarios o contratistas que desarrollen actividades que generan impacto ambiental de acuerdo con lo reportado en el formato “Planificación”. El funcionario designado como apoyo del PIGA realizará un seguimiento para verificar la efectividad de los mismos a través de las evidencias de minimización de la probabilidad o la disminución del impacto.

5.7. RIESGO DE LA/FT/FPADM - LAVADO DE ACTIVOS, Y FINANCIACIÓN DEL TERRORISMO Y FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA.

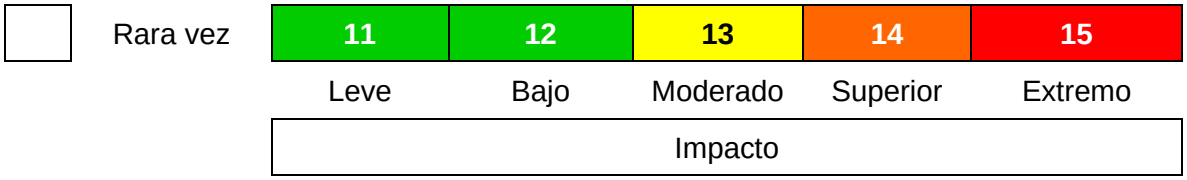
5.7.1. Etapa de Identificación

Para la identificación de los riesgos de Lavado de Activos y Financiación del Terrorismo, **SECRETARÍA DISTRITAL DE HACIENDA** toma como base el estándar colombiano ISO 31000 y el estándar australiano AS/NZS 4360, y se utilizan herramientas y técnicas con enfoque en los diferentes procesos que se ejecutan en la organización.

La matriz colorimétrica establecida para ubicar los riesgos identificados tiene una estructura de cinco (5) niveles de probabilidad y cinco (5) niveles de impacto, de acuerdo con el esquema que se presenta a continuación:

Ilustración 9. Mapa de Calor de Riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva

Probabilidad						
	Casi seguro	51	52	53	54	55
	Probable	41	42	43	44	45
	Posible	31	32	33	34	35
	Improbable	21	22	23	24	25



De acuerdo con el resultado de los valores obtenidos en la ecuación anterior, los riesgos serán ubicados en la matriz de riesgo inherente o residual, donde se evaluará el nivel de riesgo de cada uno de los factores de riesgo. Dicho nivel de riesgo se clasifica a través de unas escalas de severidad, tal como se presenta en la siguiente tabla:

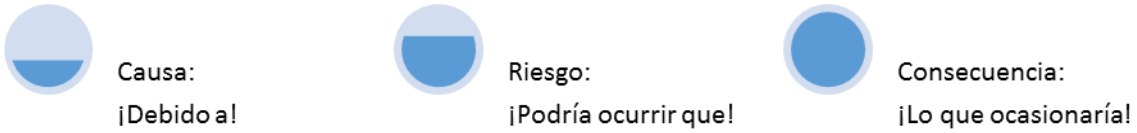
Tabla 13. Niveles de riesgo

Nivel	Escala
Extremo	4
Alto	3
Moderado	2
Bajo	1

Para cada uno de los procesos y/o procedimientos de la entidad, se procede a la identificación de los riesgos junto con su clase, factor y riesgo asociado. Posteriormente, se documentan las causas y consecuencias que pueden ocasionar los riesgos que se materialicen en el proceso evaluado.

Con el propósito de realizar una mejor redacción de los riesgos, como punto de apoyo se puede utilizar la siguiente estructura:

Ilustración 10. Estructura de redacción de los riesgos de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva



5.7.2. Etapa de Medición (Perfil de riesgo inherente)

Una vez concluida la etapa de identificación de los riesgos, continua la etapa de medición en la cual se determina la frecuencia (probabilidad) de ocurrencia del riesgo frente a cada uno de los factores o fuentes generadoras del mismo y, el impacto en caso de materializarse (para lo cual se tienen en cuenta los riesgos asociados), dichas mediciones son de carácter cualitativo y/o cuantitativo.

El resultado del cruce entre la frecuencia y el impacto permite conocer el nivel de riesgo. La medición de los riesgos se realiza a través de estimaciones objetivas (en caso de tener mediciones y datos históricos), que para el caso de la probabilidad se tiene en cuenta la frecuencia de ejecución de la actividad que genera el riesgo y el número de materializaciones del mismo, mientras que para el impacto se tienen en cuenta diferentes tipos de impacto: Financiero, Operativo, Legal, Reputacional y Contagio.

Al no disponerse de datos de frecuencias e impactos confiables o relevantes, la medición se puede realizar a través de estimaciones subjetivas por parte de los responsables de los procesos y a juicio experto del Oficial de Cumplimiento.

5.7.2.1. Determinar la probabilidad

Para determinar la probabilidad se tendrán en cuenta criterios cualitativos y cuantitativos, basados en la posibilidad de ocurrencia o en el registro del número de eventos reportados entre uno (1) y tres (3) años atrás.

A través del siguiente criterio se procede a medir la probabilidad; los rangos de probabilidad en los cuales puede ubicarse el riesgo son: Rara Vez, Improbable, Posible, Probable y Casi Seguro. Cada uno de estos niveles está asociado a intervalos de porcentaje de ocurrencia tal como se presenta en la siguiente tabla:

Tabla *14*. Determinación de probabilidad para riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva
entre uno (1) y tres (3) años

NIVEL		PROBABILIDAD CUALITATIVA	PROBABILIDAD POR EVENTO	PROBABILIDAD PORCENTUAL
5	Casi Seguro	Se espera que evento ocurra en la mayoría de las circunstancias.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último mes	Se espera la ocurrencia del evento en más del 20% de los casos
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último semestre	El evento ocurrirá entre el 15% y el 20% de los casos
3	Posible	El evento podría ocurrir en varios casos.	Existe evidencia de que el evento se ha presentado por lo menos una vez en el último año	El evento ocurrirá entre el 10% y el 15% de los casos
2	Improbable	El evento puede ocurrir en algún momento.	Existe evidencia de que el evento se ha presentado por lo menos una vez en los últimos 2 años	El evento ocurrirá entre el 5% y el 10% de los casos

NIVEL		PROBABILIDAD CUALITATIVA	PROBABILIDAD POR EVENTO	PROBABILIDAD PORCENTUAL
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (Poco comunes o anormales).	Existe evidencia de que el evento se ha presentado por lo menos una vez en los últimos 3 años	El evento puede ocurrir en menos del 5% de los casos

Tabla *15*. Determinación del nivel de probabilidad para riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva para tres (3) años

NIVEL		RANGO	VECES
5	Casi Seguro	[20% - 100%]	Más de 7,2 veces C/3 años (>7,2/36)
4	Probable	[15% - 20%)	7,2 veces C/3 años (7,2/36)
3	Posible	[10% - 15%)	5,4 veces C/3 años (5,4/36)
2	Improbable	[5% - 10%)	3,6 veces C/3 años (3,6/36)
1	Rara vez	[0% - 5%)	1,8 vez C/3 años (1,8/36)

5.7.2.2. Medir los tipos de impacto

Para medir la variable de impacto, se deben estimar los 5 diferentes tipos de impacto que podría llegar a generar un riesgo en caso de materializarse. Cada variable puntúa dentro de un modelo de asignación, y la calificación total se obtiene de una ponderación. Los 5 tipos son:

i. Financiero o Económico: en caso de pérdida económica el cual es valorado en SMMLV.
ii. Operativo: analizar la interrupción de los diferentes procesos afectando la continuidad de los mismos a nivel interno o de otras entidades del estado.
iii. Legal: tiene que ver con incumplimientos contractuales, legales y repercusiones con los entes de control.
iv. Reputacional: nivel de divulgación de los casos (interno/externo) que podría afectar la imagen de la entidad.
v. Contagio: calidad de las contrapartes que contagian a la empresa (usuarios, proveedores, funcionarios y administradores).

5.7.2.2.1. Impacto Financiero o Económico

Para medir el impacto financiero se definieron cinco (5) intervalos, los cuales están asociados al impacto sobre el patrimonio de la entidad y se asigna un porcentaje entre el 20% y el 100%. Las escalas definidas para medir el impacto financiero de la entidad es la siguiente:

Tabla 16. Determinación de impacto financiero para riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva

Nivel	Calificación	Afectación en SMMLV
Catastrófico	100%	> a 500 SMLMV
Mayor	80%	> 100 y <= 500 SMLMV
Moderado	60%	> 50 y <= 100 SMLMV
Menor	40%	> 10 y <= 50 SMLMV
Leve	20%	<= 10 SMLMV

Es de aclarar que el impacto financiero o económico se debe medir en función del monto expuesto por cada uno de los eventos de riesgo con probabilidad de materialización.

5.7.2.2.2. Impacto Operativo

El impacto operativo se mide en función de la materialización de un evento de riesgo y la interrupción que este genere en la operatividad y funcionalidad del proceso. En este orden de ideas, la escala que se genera es:

Tabla 17. Determinación de impacto operativo para riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva

Nivel	Calificación	Tiempo de reproceso
Catastrófico	100%	>5 días
Mayor	80%	>3 y <=5 días
Moderado	60%	>2 y <=3 días
Menor	40%	>1 y <=2 días
Leve	20%	0 y <=1 día

5.7.2.2.3. Impacto Legal

El impacto legal corresponde a la magnitud de la consecuencia de la materialización del riesgo en términos de incumplimiento legal y/o contractual:

Tabla 18. Determinación de impacto legal para riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva

Nivel	Calificación	Consecuencia legal y/o contractual
Catastrófico	100%	Intervención (Plan de saneamiento) de la entidad por parte de un órgano de control u otro regulador.
Mayor	80%	Multas o sanciones administrativas para la entidad por parte de entes de inspección, vigilancia y/o control.
Moderado	60%	Demandas a la entidad por parte de tercero ante jueces de lo contencioso administrativo.
Menor	40%	Investigaciones, sanciones, inhabilidades, entre otras, de tipo disciplinario, fiscal y/o penal en contra

		de alguno(s) de los funcionarios de la entidad.
Leve	20%	Ninguno, hallazgos administrativos, observaciones o recomendaciones producto de auditorías

5.7.2.2.4. Impacto Reputacional

El impacto reputacional corresponde a la magnitud del nivel de divulgación que puede generar la materialización de un riesgo de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva:

Tabla 19. Determinación de impacto reputacional para riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva

Nivel	Calificación	Nivel de divulgación
Catastrófico	100%	Afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido en medios de comunicación a nivel local y/o país
Mayor	80%	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Entidades distritales), respecto al cumplimiento de sus objetivos
Moderado	60%	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Contribuyentes), respecto al cumplimiento de sus objetivos
Menor	40%	Afecta la imagen de la entidad internamente (entre sus funcionarios y Directivos), y el tema es abordado en Comités Directivos y otras instancias internas
Leve	20%	No hay una afectación relevante a la imagen de la entidad

5.7.2.2.5. Impacto de Contagio

El impacto de contagio corresponde a la magnitud del alcance de la situación que puede generar la materialización del riesgo analizado:

Tabla 20. Determinación de impacto reputacional para riesgo de Lavado de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva

Nivel	Calificación	Nivel de alcance

Catastrófico	100%	Generado por un representante del Gobierno o Administración del Distrito Capital o funcionarios de alto nivel
Mayor	80%	Generado por un servidor de nivel medio o contratistas de alto impacto de la SDH
Moderado	60%	Generado por un servidor de bajo nivel o contratistas de bajo impacto de la SDH
Menor	40%	Generado por un contribuyente
Leve	20%	No genera contagio o causado por un tercero interesado

5.7.2.2.6. Determinar el impacto total

A cada calificación de impacto (Leve, Menor, Moderado, Mayor y Catastrófico), se le asigna un porcentaje (20%, 40%, 60%, 80% y 100%, respectivamente), sin embargo, para determinar la calificación final, ésta se define de acuerdo con la mayor calificación obtenida en cualquiera de los tipos de impacto (Financiero, Operativo, Legal, Reputacional y Contagio).

5.7.2.2.7. Riesgo inherente

Finalmente, habiendo obtenida la calificación de estas dos variables como son la probabilidad y el impacto del riesgo, debemos remitirnos al mapa de calor, que es la matriz que relaciona estas dos variables y en la que se identifica la calificación final del riesgo, en cuatro posibles niveles:

Ilustración 11. Niveles de riesgo

El propósito de la evaluación del riesgo inherente es tomar decisiones con el fin de determinar si necesitan algún tipo de control o tratamiento de acuerdo con las prioridades de la **SECRETARÍA DISTRITAL DE HACIENDA**.

La SDH definió la siguiente escala de complejidad de tratamiento de acuerdo con nivel de riesgo inherente:

Tabla *20*. Complejidad del tratamiento según Nivel de Riesgo

Nivel de riesgo	Nivel	Complejidad del tratamiento
Extremo	4	Fuerte
Alto	3	Fuerte

Moderado	2	Medio
Bajo	1	Básico

5.7.3. Etapa de Control

El propósito de esta evaluación es analizar las características claves de cada uno de los controles, así como también estimar en qué grado el control afecta la calificación inicial de la probabilidad y/o del impacto.

Una vez estimado el nivel de riesgo inherente de la actividad, con su respectiva probabilidad e impacto, se procede a identificar aquellos controles que mitigan al riesgo, de tal manera que se reduzca la probabilidad de ocurrencia y/o se disminuya el impacto que tenga (en cualquiera de los aspectos), en caso de materializarse. Esta identificación de controles se realiza a partir de controles ya existentes en la actualidad del proceso.

Los controles implementados garantizan que todos los riesgos identificados, valorados y evaluados, cuenten con un tratamiento adecuado sobre el mismo. De encontrarse riesgos que no cuenten con controles que los mitiguen adecuadamente, se realizarán planes de acción para mejorarlos y con la ayuda de los dueños de los procesos, se definirán los nuevos riesgos para ser implementados previa aceptación del Oficial de Cumplimiento y del máximo Órgano Social.

5.7.3.1. Evaluación del diseño de los controles

Una vez identificados los controles, se procede a identificar sus características con el propósito de conocer su estructura:

En esta etapa se establecen medidas para mitigar el riesgo inherente identificado y realizar tratamiento a los riesgos residuales que superen el nivel de tolerancia establecido por la entidad en la Política de Administración de Riesgo y Cumplimiento.

Luego de determinado el riesgo inherente, se deben establecer controles orientados a reducir la probabilidad de ocurrencia y/o el impacto del riesgo identificado. Para su descripción se deben tener en cuenta los siguientes elementos:

- El responsable de ejecución, que será la persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso.
- Establecer la acción, es decir, el cómo se va a ejecutar el control, mediante un verbo en infinitivo, ejemplo, revisar, validar, verificar, corroborar, conciliar, comparar, cotejar.
- Definir el complemento, es decir, los requisitos necesarios y tareas adicionales para ejecutar el control.

Para surtir esta etapa se necesita, definir una serie de atributos que permitirán establecer si el diseño del control es o no, adecuado, los atributos son:

Tipo de control: Para clasificar el control debe identificarse en qué momento dentro de la ejecución del proceso éste se activa, lo cual permitirá determinar su tipología, que puede ser preventivo, detectivo o correctivo.

Naturaleza del control: Corresponde a la forma de ejecución del control, permite establecer si éste depende de una persona (manual), de un sistema (automático), o combinado.

Documentado: Aquí debe determinarse si el control se encuentra documentado. Se considera documentado cuando existe en algún documento del Sistema de Gestión de Calidad, alguna norma (ley, decreto, resolución interna o externa, circular, memorando) u otro tipo de documento tal como política, acta de comité, etc.

5.7.3.2. Evaluación de la efectividad de los controles

Posteriormente, el método para evaluar la efectividad de los controles se califica de acuerdo con las siguientes características como la (i) ejecución del control, (ii) la frecuencia con la que se ejecuta, (iii) el nivel de mitigación esperado y (iv) el nivel de incertidumbre sobre esa mitigación esperada.

a. **Oportuno:** Para establecer la oportunidad, es necesario identificar si la periodicidad del control es consistente o coincide con la frecuencia de ejecución de la actividad en la cual podría generarse el riesgo.

b. **Evidencia:** Es todo aquello que permita probar la ejecución del control y aquí se determina si el control cuenta o no con evidencia.

Información adicional de los controles

a. **Frecuencia:** Corresponde a la periodicidad de ejecución del control, que puede ser diaria, semanal, quincenal, mensual, bimestral, trimestral, cuatrimestral, semestral, anual, continua (funciona de manera permanente, ininterrumpida, pero su activación se da por una condición, por ejemplo, los controles de seguridad física o lógica) y esporádica (el control se ejecuta por demanda, por ejemplo, los controles correctivos que comúnmente se ejecutan después de ocurrida la falla).

b. **Evidencia**: El detalle de la evidencia específica del control, es decir la forma en la que va a demostrarse que se ejecutó el control, por ejemplo, formato diligenciado, comunicación, correo electrónico, marca en un aplicativo, archivos en diferentes formatos.

c. **Responsable:** Se debe indicar el cargo del responsable asignado para su ejecución.

Por último, se estima la efectividad del control mediante los pesos ponderados de cada característica y se realiza una extrapolación lineal de este resultado.

La determinación del nivel de efectividad del control se realiza de acuerdo con su nivel de calificación, tal como se indica en la siguiente tabla:

Tabla *21*. Determinación del nivel de efectividad del control

Nivel	Indicador	Calificación
Fuerte	5	[80%-100%]
Moderado	4	[60%-80%)
Débil	1	[0%-60%)

5.7.3.3. Etapa de valoración del riesgo residual (Perfil de riesgo residual)

El riesgo residual es el remanente de riesgo que queda después de haber tenido en cuenta y calificado los controles actuales del proceso. Es importante advertir que el nivel de riesgo al que está sometido **SECRETARÍA DISTRITAL DE HACIENDA** no puede erradicarse completamente, por tanto, quedará para cada riesgo un nivel de riesgo residual el cual la compañía debe decidir aceptar o no.

Una vez obtenida la calificación final del riesgo inherente se diseñan, se evalúan y aplican los controles pertinentes a la actividad, con el fin de reducir su probabilidad y/o impacto.

Para identificar la fuerza de desplazamiento del riesgo inherente (reducción de una o ambas variables), por política se definió que la mitigación del riesgo de acuerdo con la calificación de los controles, tanto para la probabilidad como para el impacto, disminuirá de conformidad a la siguiente tabla:

Tabla *22*. Desplazamiento del nivel de riesgo de acuerdo con la evaluación del conjunto de controles

EVALUACIÓN DEL CONJUNTO DE CONTROLES			DESPLAZAMIENTOS
Promedio del conjunto de controles	Fuerte	81%-100%	2
	Moderado	61%-80%	1
	Débil	0%-60%	0

Como resultado de esta etapa, el control debe traducirse en la disminución de la posibilidad de ocurrencia y/o del impacto en caso de presentarse, cuando el control es preventivo o detectivo, disminuye la probabilidad y cuando éste es correctivo, disminuye el impacto.

5.7.3.4. Etapa de tratamiento

Después de establecido el riesgo residual, debe determinarse el tratamiento de los riesgos, que no es otra cosa que la toma de decisiones frente a los resultados obtenidos. El tratamiento debe realizarse de acuerdo con lo establecido en la política de administración de riesgos y cumplimiento.

- **Mitigar:** Se implementan acciones que disminuyen el riesgo.

- **Transferir o compartir:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia (aseguradoras o contratistas). Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

- **Evitar o eliminar:** se eliminan aquellas actividades dentro del proceso que pueden dar origen a un riesgo.

- **Aceptar:** Se asume el riesgo conociendo las consecuencias que traería su materialización.

  De llegar a presentarse casos excepcionales en los cuales se identifiquen riesgos que ante la capacidad de mitigación actual de la Entidad no sea posible ubicarlos en los niveles de riesgo tolerables, éstos deberán ser aceptados de manera expresa por parte de los responsables del proceso y con el aval de la Alta Dirección y el comité de riesgos.

5.7.4. Etapa de monitoreo

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo está a cargo del Oficial de Cumplimiento y su propósito principal des el de aplicar, sugerir correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.

Una vez diseñado y validado el plan para administrar los riesgos, anualmente, la OACR verifica la efectividad de los controles establecidos en las matrices para la mitigación de los riesgos de LA/FT/FPADM y sus riesgos asociados, para asegurar que estos sean apropiados y funcionen correctamente. Este ejercicio se realiza mediante la recolección de evidencias, las cuales permiten evaluar y calificar cada uno de los controles. Como resultado de lo anterior, se generan conclusiones y recomendaciones generales. En caso de ser necesario, se pueden realizar actualizaciones en las matrices de riesgo. Esta actividad se encuentra documentada en el procedimiento Monitoreo de controles de riesgo en procesos 123-P-02.

6. GLOSARIO

Aceptar: Se asume el riesgo conociendo las consecuencias que traería su materialización.

Activo de información: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Administración de riesgo: proceso de identificación, medida y administración de los riesgos que amenazan la existencia, los activos, las ganancias o al personal de una organización, o los servicios que ésta provee.

Amenaza: posibilidad de que un sistema vulnerable sea atacado y sufra daños.

Basilea: acuerdos o recomendaciones internacionales de supervisión bancaria, emitidos por el Comité Internacional de supervisión Bancaria (CBSB - Basel Committee on Banking Supervision).

BCM: Gestión para la "Continuidad del Negocio" las acciones y actividades que desarrollan la capacidad de una organización o empresa para sobrevivir a acontecimientos extraordinarios y que pueden tener un impacto negativo en la misma.

BCP: Un plan de continuidad del negocio (*BCP por sus siglas en inglés*) es un documento que describe cómo una empresa seguirá funcionando durante una interrupción no planificada del servicio.

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

Clasificación de riesgo: permite agrupar los riesgos identificados en categorías.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Contexto: es la combinación de cuestiones internas y externas que pueden tener un efecto en el enfoque de la empresa según el desarrollo y la consecución de sus objetivos.

Contingencia: Una contingencia se refiere a actividades o eventos que ocurren más allá del rango normal de operaciones organizacionales.

Continuidad del Negocio: estrategias y planificación mediante las cuales las organizaciones se preparan para dar respuesta a eventos catastróficos tales como incendios, inundaciones, ataques cibernéticos, accidentes o errores humanos.

Control: Medida que permite reducir o mitigar un riesgo.

Control correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Atacan el impacto frente a la materialización del riesgo.

Control detectivo: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Atacan la probabilidad de ocurrencia del riesgo.

Controles administrativos: Hace referencia al establecimiento de controles a partir de procedimientos, manuales, instructivos ejemplos, señalizaciones, toma de temperatura, control de acceso.

Controles de ingeniería: Consiste en el diseño de controles en sitio que reduzcan el nivel de riesgo.

Control Preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo.

COSO: (Committee of Sponsoring Organizations of the Tradeway Commission) es una organización compuesta por organismos privados, establecida en los EE. UU., dedicada a proporcionar un modelo común de orientación a las entidades sobre aspectos fundamentales de: gestión ejecutiva y de gobierno, ética empresarial, control interno, gestión del riesgo empresarial, control del fraude, y presentación de informes financieros**.**

Daños a activos fijos/ eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

DRP: estrategia y acciones para seguir para restablecer los servicios de TI ante cualquier eventualidad en tiempos muy cortos y sin pérdida de información.

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

Eliminación: Consiste en eliminar la fuente del riesgo.

Equipos y elementos de protección personal: Consiste en la entrega de elementos de protección a los servidores requeridos para la ejecución de sus labores con el propósito de reducir su exposición al riesgo.

Evento de riesgo: situación que ocurre en un lugar particular, durante un intervalo de tiempo y que tiene un impacto en algún proceso o la realización de algún producto o servicio en la entidad.

Evitar: se eliminan aquellas actividades dentro del proceso que pueden dar origen a un riesgo.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Fallas tecnológicas: Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Fraude externo: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude interno: Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Identificación: etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el

que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Líneas de defensa: permiten identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad.

Mapa de calor: punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

Matriz DOFA: Herramienta utilizada para la definición del contexto dentro de la organización.

MIPG: marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión Institucional.

Mitigar: Se implementan acciones que disminuyen el riesgo.

Monitoreo: proceso continuo y sistemático mediante el cual se verifica la eficiencia y la eficacia de la gestión de riesgos.

Nivel de deficiencia: Magnitud de la relación esperable entre (1) el conjunto de peligros detectados y su relación causal directa con posibles incidentes y (2) con la eficacia de las medidas preventivas existentes en un lugar de trabajo.

Nivel de exposición: Situación de exposición a un peligro que se presenta en un tiempo determinado durante la jornada laboral.

Peligro: Fuente, situación o acto con potencial de daño en términos de enfermedad o lesión a las personas, o una combinación de estos.

Política de Administración de Riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Relaciones laborales: Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo Operacional: posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgos Ambientales: posibilidad de que por forma natural o por acción humana se produzca daño en el medio ambiente.

Riesgos de Seguridad y Salud en el Trabajo: Se entenderá como «riesgo laboral» la posibilidad de que un trabajador sufra un determinado daño derivado del trabajo. Para calificar un riesgo desde el punto de vista de su gravedad, se valorarán conjuntamente la probabilidad de que se produzca el daño y la severidad de este. Son los riesgos existentes en el área laboral los que pueden derivar una enfermedad laboral o en un accidente de trabajo.

Sustitución: Consiste en sustituir la fuente de peligro por un material menos peligroso o reducir la energía del sistema que cumpla la misma función minimizando el peligro.

Transferir: Se terceriza el proceso o traslada el riesgo a través de seguros o pólizas, con lo cual la responsabilidad económica cae en el tercero más no la responsabilidad reputacional.

Usuarios productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

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

7. CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCIÓN DE CAMBIOS
1	**7/07/2022**	N/A
2	19/06/2024	Se actualiza el nombre del Manual para la Administración de Riesgo No Financiero de la Secretaría Distrital de Hacienda, a Manual para la Administración del Riesgo en Procesos. Numeral 1. Introducción de nuevos elementos del Sistema de Administración de Riesgos. Se agregó el numeral 4. Apetito de riesgo, conforme a la Política de Administración de Riesgos y Cumplimiento. Numeral 5. Se agregó ilustración de las Etapas de la Administración del Riesgo. Numeral 5.3. Riesgo Operacional Actualización de las tablas de Probabilidad e Impacto. Actualización de la etapa de “Control” reorganizándose las actividades y describiendo con mayor profundidad esta etapa.

		Actualización del Tratamiento de Riesgos conforme a lo descrito en la Política de Administración de Riesgos y Cumplimiento. Numeral 5.4. Continuidad del Negocio; Se actualizan los factores de riesgo Numeral 5.4.2 Se actualiza la tabla 20 Incluyendo nuevos escenarios de interrupción Actualización tablas 21 y 22 de Probabilidad e Impacto. 5.4.3 Se elimina el concepto de Plan de Contingencia y se unifica con el plan de Continuidad Literal b. Se elimina el Plan de Recuperación de Desastres Literal c. se actualiza el concepto de ejercicios de continuidad Literal d. se actualiza el concepto de capacitación y sensibilización Literal f. se elimina el inciso de mejora continua el cual se traslada al procedimiento de Administración de Riesgos. Actualización del glosario. Actualización de la numeración para visibilizar las etapas de la administración de los riesgos en la SDH. Se ajusta el término “riesgo no financiero” al de “riesgo en procesos” a nivel general en el documento. Se asocial el MN-9 al CPR-123 dada la reorganización de los documentos del SGC bajo el enfoque de macroproceso.

8. APROBACIÓN

ELABORÓ/ACTUALIZÓ (Nombre y Cargo)	REVISÓ (Nombre y Cargo)	APROBÓ (Nombre y Cargo)
Profesionales OACR: Beverly Carolina Ramírez Triana Ivonne Andrea Torres Cruz Danilo Santamaría Gómez **Contratista experto en Sarlaft:** Carlos Andrés Lancheros	**Asesores OACR:** Karyme Baquero Orozco Juan Gabriel Prieto Otavo **Contratista experta continuidad de negocio:** Sandra Milena Velásquez Vera **Profesional OACR:** Carol Andrea Hernández Bohórquez	Paola Castillo Ariza (Jefe OACR)