MANUAL OPERATIVO
ADMINISTRACIÓN DEL RIESGO

Control de Versiones

Versión	Fecha	Descripción Modificación	Folios
15	**2025-02-12**	- **Esta vesión incorpora los ajustes aprobados por el Comité Institucional de control Interno (18-12-2024) en cuanto a la actualización de la Política de Riesgos, los objetivos de riesgos y los tipos de riesgos que asume el IDU.**	**29**
14	2024-11-28	- Ajuste introducción. - Ajuste al capítulo de normatividad. - Inclusión de criterio para seguimiento a la política de riesgos - Ajuste a los niveles del mapa de riesgos. - Inclusión de tipología de causas para riesgos de corrupción. - Inclusión de otros tipos de consecuencias del riesgo (se incluye daño fiscal y derechos fundamentales). - Aclaraciones para cálculo de la probabilidad y del impacto. - Se elimina el capítulo de líneas de defensa (Se trasladó en un documento independiente). - Ajustes en redacción y forma.	28
13	2022-05-02	- Ajuste en la política de administración de riesgos y objetivos del riesgo según aprobación del comité Institucional de Control Interno (ICI). - Aprobación por parte del Comité ICI del apetito de riesgo y nivel de tolerancia al riesgo. - Se suprime la opción de tratamiento “Compartir”. Acción ya contemplada dentro de la opción de tratamiento de “Reducir”	31
12	2021-12-10	- Alineación a los criterios requeridos por la Guía versión 5 de Administración de Riesgo del DAFP. - Inclusión del concepto de apetito y tolerancia del riesgo - Se incluye el contenido del documento de la Política de Riesgos (Documento que se elimina) - Se incluye ajuste del capítulo de Líneas de Defensa (Se elimina el documento de líneas de Defensa). - Ajustes en el método de evaluación de riesgos - Se modifica el método de valoración de controles	31
11	2021-09-29	Se incluye lineamientos para asignación y aceptación del Dueño de Riesgos para seguridad de la información.	26
10	2020-04-13	Se describe con mayor detalle los lineamientos para la gestión de los riesgos de seguridad de la información. Se describen los criterios para tener en cuenta para la gestión de eventos de riesgos materializados. Se realiza una mejora en la descripción de las etapas de administración del riesgo. Y se especifica dentro de las estrategias de tratamiento del riesgo la de “Compartir”.	26
9	2019-05-31	La versión 9 se motiva en cumplimiento a lo requerido por el Modelo Integrado de Planeación y Gestión MIPG y lo establecido en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas del DAFP (agosto de 2018). Se hace una referencia para la administración del riesgo de soborno.	29
8	28-Sep-2018	Se modifica el objetivo y alcance del manual. La etapa de Valoración del Riesgo se modifica por Evaluación del Riesgo. Se modifica el capítulo de gestión de eventos de Riesgo Materializados incluyendo la directriz de reporte de eventos junto con el seguimiento cuatrimestral. Se establece la modificación en la matriz de riesgos de gestión para incluir los campos de seguimiento. Se modifica el capítulo de monitoreo ahora denominado Seguimiento y Monitoreo para ejecutar el seguimiento de los riesgos de gestión junto con los riesgos de corrupción. Dado que se amplía la descripción del capítulo de gestión de eventos de riesgo materializados, ya no es necesario continuar con la guía de riesgos materializados GUPE21 por lo que se elimina del manual de procesos del IDU junto con el formato de eventos de riesgo FOPE11.	29

Versión	Fecha	Descripción Modificación	Folios
7	Res. 1080 27-Mar-2018	Ajuste del marco normativo (por aplicación del modelo MIPG). Se ajustan descripción de las escalas de probabilidad. Ampliación de la descripción de los controles y referencia específica al Dueño del riesgo Se incluyen los criterios para gestión de oportunidades. Se elimina el capítulo de Responsabilidades, por cuanto están contempladas en la descripción de las etapas de administración de riesgos.	22
6	Res. 2958 15-Jun-2017	Se ajusta la introducción, trayendo el análisis sobre la toma de decisiones descrita antes como un capítulo del manual. Se ajusta el objetivo y alcance. Se Incluye la normatividad expedida desde el 2014 a la fecha de publicación de este manual. Se ajusta la metodología de calificación de los riesgos y los controles. Se referencia al documento de política de riesgos (sin incluirla como tal). Se incluye los mecanismos y referencia para la gestión de riesgos materializados.	23
5	Res. 576 3-Feb-2014	Se incluye la Política y los Objetivos de Riesgos. Se alinea la metodología para los diferentes tipos de riesgos; de corrupción, en seguridad de la información y en la contratación. Se mejora la descripción de las etapas, se modifican los criterios en el nivel del riesgo, se ajusta la normatividad que le aplica, se mejoran los términos y definiciones, se define responsabilidades para la gestión del archivo de las matrices y se presentan mejoras conforme a los estándares de documentación.	24
4	Res. 445 16-Feb-2012	Se realizan ajustes en generalidades, escalas y criterios de calificación y aceptación del riesgo, se incluyen formatos para etapas de la administración del riesgo. Y en general se ajusta redacción de cada una de las etapas de administración del riesgo y de los responsables.	45
3	No. Ac. Adm.313 16-Feb-2010	Se actualiza teniendo en cuenta la nueva estructura institucional	63
2	No. Ac. Adm. 5139	Se actualiza el alcance de la Administración del Riesgo en el Instituto de Desarrollo Urbano, las fórmulas de cálculo de probabilidad, las responsabilidades de la Subdirección Técnica de Desarrollo de la Organización	62
1	No. Ac. Adm. 6896	Adopción del documento	63

El documento original ha sido aprobado mediante el SID (Sistema Información Documentada del IDU). La autenticidad puede ser verificada a través del código

Participaron en la elaboración[1]	**John Alexander Quiroga Fuquene, OAP /**
Validado por	**Liliana Pulido Villamil, OAP Validado el 2025-02-12**
Revisado por	**Liliana Pulido Villamil, OAP Revisado el 2025-02-12**
Aprobado por	**Liliana Pulido Villamil, OAP Aprobado el 2025-02-12**

[1] el alcance de participación en la elaboración de este documento corresponde a las funciones del área que representan.

CONTENIDO

INTRODUCCIÓN

Cuando se tiene la misión de gestionar un proceso, proyecto o una simple actividad se involucran aspectos asociados a la incertidumbre y a situaciones que no siempre están bajo el control de la administración y que si no se analizan y gestionan podrían afectar considerablemente el logro de los objetivos propuestos. El concepto del riesgo y su administración pretende abordar dichos aspectos con el propósito de generar mayor confianza en la consecución de los resultados.

La efectividad para enfrentar dichas situaciones se encuentra generalmente condicionada al mayor o menor grado de información que posea acerca de los factores asociados y su contexto.

La propuesta actual es invitar a cada nivel de la Entidad a generar un espacio formal y sistemático en el cual, de manera metódica y con suficiente información, se evite caer en la tentación de la intuición, y se plantee un modelo de administración del riesgo que prevenga los aspectos negativos y se potencialicen las oportunidades, que facilite el logro de los resultados deseados.

Desde el año 2002, el Instituto de Desarrollo Urbano, en cumplimiento de la obligación ha venido trabajando en el proceso de administración del riesgo que responda a las cambiantes necesidades de la Administración Pública. Fruto de la evolución de este tema, se decide elaborar el Manual de Administración del Riesgo, con el cual se espera dar los lineamientos necesarios para atender los temas relacionados con el manejo de la incertidumbre y el riesgo en la gestión administrativa.

La Administración del Riesgo hace parte de la gestión administrativa y debe entenderse como una práctica preventiva de obligatorio cumplimiento por parte de todos los servidores públicos y contratistas vinculados.

Encontrará en este manual una metodología descrita en 8 etapas de administración del riesgo; contexto estratégico, identificación, análisis, valoración, tratamiento, monitoreo, comunicación y gestión de eventos materializados, aplicada a los diferentes tipos de riesgo asociados al modelo de procesos del IDU, con algunas diferencias metodológicas dependiendo del tipo de riesgos ya sea por algún requisito específico establecido en la normatividad o necesario para su adecuada gestión. el manual determinará los instrumentos y la forma de aplicación para cada caso.

Desde la versión 7 del manual se incluyen los criterios para gestionar las oportunidades; como enfoque preventivo y eficiente que facilite la obtención de los objetivos institucionales en el marco del sistema de gestión de la calidad.

El manual de riesgos toma como fundamento metodológico el estándar ISO 31000:2018 respecto de las directrices generales para gestionar los riesgos en una organización y considera los lineamientos expuestos para las entidades públicas en la guía para administración de riesgos del DAFP. Sin embargo, en algunos aspectos la metodología IDU adapta el proceso de gestión del riesgo y sus instrumentos para dar cumplimiento a la política de riesgos y el apetito establecido por la Alta Dirección.

1 OBJETIVO

Definir lineamientos y criterios para gestionar los riesgos y oportunidades que permitan generar confianza en el cumplimiento de los objetivos del Instituto.

2 ALCANCE

La gestión del riesgo debe ser aplicable a todos los procesos de gestión establecidos en la Entidad y para todos los riesgos de acuerdo con el apetito y tolerancia al riesgo del Instituto.

3 MARCO NORMATIVO

- Ley 2195 de 18 de enero de 2022, “Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones”.

- Decreto 1499 del 11 de septiembre de 2017, "Por medio del cual se modifica el decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 1122 de agosto de 2024, “Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública”.

4 TÉRMINOS Y DEFINICIONES

Los términos y definiciones aplicables al procedimiento pueden ser consultados en el micrositio Direccionario de términos IDU (http://Intranet/web/intranet/diccionario-terminos-idu).

- Acción Correctiva
- Corrección
- Impacto
- Probabilidad
- Identificación del riesgo
- Riesgo
- Riesgo residual

5 POLÍTICA DE RIESGOS

La política de riesgos es la declaración de la Alta Dirección y las intenciones generales para una adecuada gestión de riesgo en la Entidad.

En el IDU la política es revisada y aprobada por la Alta Dirección a través del Comité Institucional de Coordinación de Control Interno. La Política deberá ser presentada por la Oficina Asesora de Planeación, y anualmente debe ser revisada su adecuación e implementación.

Descripción General de la Política de Riesgos:

> *“El Instituto de Desarrollo Urbano incorpora en su gestión las prácticas de administración del riesgo para generar valor en la ejecución de sus procesos;*

mediante un adecuado liderazgo y participación en el contexto, evaluación, tratamiento, monitoreo y comunicación de los riesgos que asume en el desarrollo de su misión. Que para una adecuada gestión del riesgo el IDU implementa los procesos de debida diligencia necesarios para el conocimiento de la contraparte, e implementa y garantiza un canal institucional para la gestión de las denuncias."

El seguimiento a la política de riesgos se realizará en el Comité Institucional de Control Interno por lo menos 1 vez al año, o con mayor frecuencia dependiendo del nivel de riesgo inherente o residual que se quiera observar y/o a solicitud del Comité Institucional de Control Interno.

5.1 TIPOS DE RIESGOS ASUMIDOS

En el marco de la política de riegos, y el apetito de riesgos del Instituto, se asumen aquellos riesgos que son necesarios gestionar para cumplir con la misión IDU y el marco legal aplicable:

1. **Riesgos de Integridad:** En cumplimiento del Programa de Transparencia y Ética Pública PTEP, el IDU identifica y gestiona los siguientes riesgos que afectan la integridad pública:

    a. **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. (Fuente Guía Administración de Riesgos del DAFP). Incluye el riesgo de soborno y riesgo de fraude.
        - **Riesgo de soborno**: Combinación de las consecuencias y la probabilidad de un evento de soborno.

        Soborno: Aceptar, solicitar, prometer, ofrecer o entregar, por parte de un colaborador del IDU, o de un externo, en forma directa o indirecta, cualquier beneficio (financiero o no) como incentivo o recompensa para que una persona cumpla o deje de cumplir en relación con sus funciones u obligaciones.
        - **Riesgo de Fraude**: Es la posibilidad de incurrir en pérdidas económicas, reputacionales u operativas por la comisión de un fraude afectando los intereses del Instituto.

        Fraude: Acción deliberada, en contra de lo que es verdadero o legal y que perjudica la gestión pública y/o el patrimonio público.

    b. Riesgo por conflicto de interés. Posibilidad de incurrir en pérdidas por acciones invalidadas por la comisión de un conflicto de interés en las actuaciones administrativas que se desarrollen en el Instituto.

    c. Riesgo LA/ FT/ FP (Lavado de Activos, Financiación de Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva):
    Posibilidad de pérdida o daño que puede sufrir la entidad por su propensión a ser utilizada directamente o través de sus operaciones como instrumento para el Lavado de Activos, Financiación del Terrorismo y/o Financiación de la Proliferación de Armas de Destrucción Masiva.

2. **Riesgo de Operativo:** Es 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.

3. **Riesgo Legal**: Probabilidad de que ocurra y las consecuencias del incumplimiento de las obligaciones establecidas en el régimen normativo aplicable. En esta definición de riesgo se consideran también los eventos de carácter exógeno, por ejemplo, riesgos jurídicos exógenos que por fallos judiciales afecten el desarrollo y ejecución de planes, programas, proyectos o procesos.

4. **Riesgo Reputacional**: La posibilidad de incurrir en pérdidas por eventos o sucesos que afecten la reputación de la entidad.

5. **Riesgo Estratégico**: Posibilidad de incurrir en pérdidas por eventos que afectan la estrategia de alto nivel de la entidad, o que por ocasión de una iniciativa estratégica la entidad vea afectado sus intereses.

6. **Riesgo de Seguridad de la Información**: Posibilidad de incurrir en pérdidas dada la combinación de amenazas y vulnerabilidad que afecten a un activo o grupo de activos de información de la Entidad, en cuanto a su confidencialidad, integridad y disponibilidad. Incluye el riesgo de seguridad digital.
    1. Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidad en el entorno digital. Puede Debilitar el logro de los objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el amiente físico digital y las personas. (Fuente Guía Administración de Riesgos del DAFP).

7. **Riesgo Contractual:** Posibilidad de que suceda algún evento que puede generar efectos adversos o positivos, y de distinta magnitud en el logro de los objetivos del proceso de contratación o en la ejecución de un contrato.
   (Fuente: Manual para la Identificación y cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente. Se adiciona “efecto positivo”)

8. **Riesgo Ambiental:** Posibilidad de que suceda algún evento que ocasione un daño ambiental o incumplimiento normativo (infracción ambiental).

   El daño ambiental hace referencia a toda pérdida, disminución, detrimento o menoscabo significativo inferido al medio ambiente; el que ocurre sobre algún elemento ambiental como consecuencia de un impacto adverso…
   (*Daño Ambiental Tomo I / Martha Isabel Gómez Lee…[et al.]. -Bogotá: Universidad Externado de Colombia 2007*)

9. **Riesgo Laboral:** Posibilidad de que ocurra un accidente laboral o se contraiga una enfermedad laboral.

   Entiéndase como accidente de trabajo todo suceso repentino que sobrevenga por causa o con ocasión del trabajo y, que produzca en el trabajador una lesión orgánica, una perturbación funcional o psiquiátrica, una invalidez o la muerte.
   La enfermedad laboral es aquella contraída como resultado de la exposición a factores de riesgo inherentes a la actividad laboral o del medio en el que el trabajador se ha visto obligado a trabajar.
   (Ley 1562 de 2012).

10. **Riesgo de Gestión del Conocimiento:** La posibilidad de incurrir en pérdidas por eventos que ocasionen fuga de capital intelectual o pérdida de conocimiento de la entidad.

11. **Riesgo Financiero.** Posibilidad de tener desvíos frente a los resultados financieros esperados en la entidad, explicados por la administración de sus inversiones, decisiones de financiación y manejo de la liquidez.

12. **Riesgo de Continuidad:** Posibilidad de incurrir en pérdidas por eventos que puedan causar interrupciones de las actividades o indisponibilidad de los recursos críticos del negocio.

13. **Riesgo Fiscal**

Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (DAFP, 2022, pág. 12)

6 OBJETIVOS DE RIESGOS

Para un adecuado despliegue de la política de riesgos en los diferentes niveles de la entidad se han establecido los objetivos de riesgos, los cuales son adoptados por la Alta Dirección a través del Comité Institucional de Control Interno.

Los objetivos en el IDU que facilitan el cumplimiento de la política de administración del riesgo son:

1. *Mantener el nivel de riesgo residual en cumplimiento del apetito y tolerancia del riesgo del Instituto.*

2. *Alinear la metodología de administración de riesgos a las disposiciones normativas y las referencias técnicas apropiadas para el Instituto.*

3. *Implementar y mantener un sistema de información que facilite el registro, monitoreo y consulta de los riesgos*

4. *Cumplir el 100% de los requisitos establecidos en el Programa de Transparencia y Ética Pública respecto de la administración del riesgo en el IDU.*

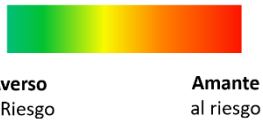
7 APETITO Y TOLERANCIA AL RIESGO

El apetito de riesgo y el nivel de tolerancia al riesgo son aprobados por la Alta Dirección a través del Comité Institucional de Control Interno y hace parte integral de la política de riesgos

El apetito de riesgo es el nivel de riesgo que la entidad puede aceptar (Fuente Guía DAFP). El apetito estará determinado por los diferentes tipos de riesgos que el Instituto deba asumir para cumplir con su misión y objetivos. Deberá el apetito considerar los requisitos normativos que existan para algún tipo de riesgo y los requisitos propios del instituto de acuerdo con el Sistema Integrado de Gestión.

Nivel de Riesgo: El nivel de riesgo es la combinación del valor de la probabilidad y el valor del impacto de un riesgo. Para el instituto esta relación estará representada por el mapa de calor y las escalas de probabilidad e impacto.

Apetito de Riesgos:
En tipos de riesgos negativos (cuya materialización trae pérdidas), la recomendación como entidad que administra recursos públicos es ser aversos a dicho riesgo y motivar su adecuado tratamiento y control para evitar su ocurrencia.

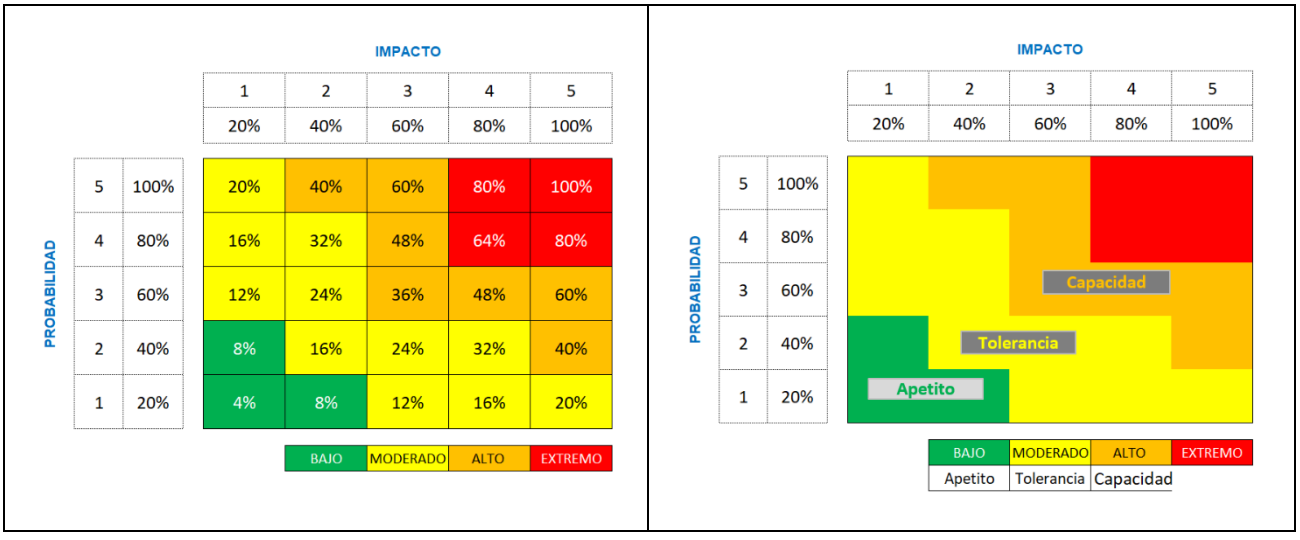


El apetito en el Instituto es que el riesgo residual se lleve a un nivel BAJO, (zona de calor verde).

Nivel de Tolerancia del Riesgo:
Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo. (Fuente Guía V5. DAFP)

Para el Instituto, la máxima desviación permitida es un nivel a partir de su apetito, es decir que el nivel de tolerancia máxima es de nivel MODERADO (zona de calor amarillo).

A continuación, se presenta el mapa de riesgos aplicable al instituto y el nivel del apetito y tolerancia:



Para riesgos de corrupción el nivel de tolerancia es 0, es decir, que no está permitido como política de tratamiento aceptar el riesgo de corrupción.

8 METODOLOGÍA DE ADMINISTRACIÓN DEL RIESGO

La Administración del Riesgo en el Instituto de Desarrollo Urbano se desarrolla en armonía con el enfoque basado en procesos que rige su operación; por lo tanto, el análisis necesario se realizará a

cada uno de los procesos y se verificará su interacción con los demás elementos del proceso de gestión tales como los objetivos estratégicos y los responsables de la gestión.

El coordinador metodológico es la Oficina Asesora de Planeación, quien definirá la metodología para la administración del riesgo y asesorará a la Alta Dirección y demás dependencias en el desarrollo de la metodología.

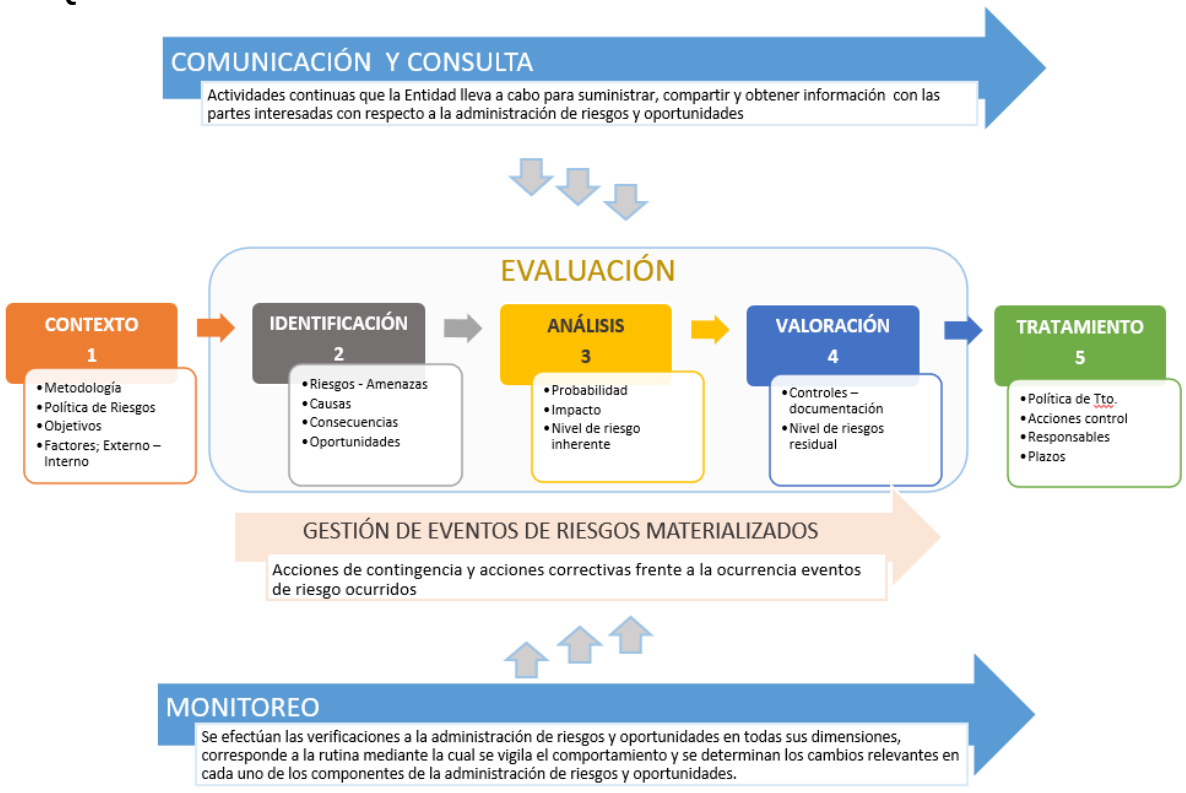
Para desarrollar la Administración del Riesgo en el Instituto, se requiere el trabajo de un equipo que conozca las actividades o procesos que serán objeto de análisis, se prefiere que dicho equipo esté constituido no sólo por el personal directo en dichas actividades, sino también por personal cuyas áreas sean clientes o proveedoras del proceso analizado.

Los responsables de la gestión del proceso son a su vez responsables de la gestión de los riesgos a los que se expone ese proceso, por consiguiente, están encargados de coordinar las actuaciones necesarias para dar cumplimiento a la identificación de los riesgos y a los planes de tratamiento que se suscriban con el fin de reducir el nivel de riesgo presente en las actividades del Instituto.

Entre mayor sea la calidad de la información empleada para la identificación del riesgo, es mayor la probabilidad de desarrollar medidas adecuadas de gestión que permitan optimizar la labor, reduciendo la incertidumbre, ampliando la posibilidad de éxito en nuevas iniciativas y orientando la gestión hacia los objetivos realmente impactantes en la organización.

La Administración del Riesgo en el Instituto de Desarrollo Urbano – IDU consta de 8 etapas, como se muestra en la siguiente figura:

ESQUEMA GENERAL DE LA ADMINISTRACIÓN DEL RIESGO Y OPORTUNIDADES



Las etapas aquí definidas están orientadas a la gestión de todo tipo de riesgo a los que se expone la entidad en el desarrollo de su misión, los criterios específicos para algunos tipos de riesgos se describirán en los capítulos siguientes.

8.1 ETAPA 1. CONTEXTO ESTRATÉGICO

Definir los activos de riesgos:
Establecer el contexto estratégico del riesgo incluye primeramente definir los activos de riesgos, es decir, los criterios y metodología para la gestión de riesgos. En el IDU, esto se registra principalmente en el documento Manual de Riesgos.

La realiza es realizada por la Oficina Asesora de Planeación (OAP) para los riesgos de gestión y de corrupción, sin embargo, para otros tipos de riesgos, donde sea otra dependencia quien ejerza el liderazgo, ella será responsable en la definición de dichos criterios, considerando siempre los lineamientos en conjunto que se definan con la OAP y en cumplimiento de la política de riesgos y el apetito de riesgos establecido por la Alta Dirección.

Conociendo el contexto interno y externo:
El contexto estratégico del riesgo debe precisar el análisis del ambiente interno y externo en el que se desarrolla el proceso objeto de análisis (o el elemento al que se le identifica riesgos). Por ejemplo, para identificar riesgos de un proceso, deberemos comprender cuál es el contexto interno y externo en el que ese proceso debe desarrollarse, ese entendimiento nos da información relevante para la gestión de riesgos.

Primeramente, comprendemos el ambiente interno de la entidad. Para ello es conveniente definir por lo menos las fortalezas y debilidades, Aquí se analizan factores como; humanos, tecnológicos, financieros, físicos, operativos y cultura organizacional entre otros.

Segundo, se define la relación entre la organización y su entorno (contexto externo). Para ello es conveniente definir oportunidades y posibles amenazas. Aquí se analizan factores económicos, políticos (percepciones públicas/ imagen), sociales, cultural, legal, reglamentario, tecnológico, ambiental, fiscales entre otros.

La información de salida de la etapa del contexto estratégico se registrará en el formato FOPE04

8.2 ETAPA 2. EVALUACIÓN

8.2.1 IDENTIFICACIÓN DEL RIESGO

El propósito de esta actividad es identificar una lista de riesgos que puedan afectar el objetivo del proceso (o elemento de análisis). Para ello es importante considerar la información resultante del contexto del proceso.

Es importante anotar que en este listado de riesgos se deben incluir no solamente situaciones que hayan ocurrido, sino aquellas que, en opinión de los analistas reunidos, tengan una posibilidad de ocurrir. Este es el enfoque del riesgo, y es pensar que podría suceder que afecte el logro de mi objetivo.

Se recomienda el uso de diferentes fuentes de información para la comprensión de los riesgos potenciales; uso de cuestionarios, revisiones de informes de auditoría, informes de quejas, análisis de eventos en entidades similares, reuniones de expertos, etc.

La descripción de riesgo debe responder a la pregunta ***¿qué puede suceder?*** Entendido como eventos potenciales asociados a la incertidumbre y que de materializarse suponen un impacto o efecto sobre el objetivo del proceso (o del sujeto análisis del riesgo).

La identificación, deberá dar cuenta de las causas del riesgo; consideradas como los factores que motivan o facilitan la ocurrencia del riesgo. La descripción de la causa responde a la pregunta frente al riesgo identificado de ***¿Cómo puede suceder?***

Para la causa principal del riesgo se deberá determinar la causa raíz. Un método sencillo para identificar la causa raíz es hacernos la pregunta *¿Por qué puede suceder la causa principal?*

Se identificarán las consecuencias de materializarse el riesgo, estas consecuencias dan cuenta de las áreas de impacto y efectos que trae la materialización del riesgo. Existen diferentes tipos de consecuencias; económicas, reputacionales, legales, operativas, fiscales, entre otras.

La redacción se debe alinearse a situaciones de carácter general y que las situaciones expresadas en las causas correspondan fielmente a los eventos generadores o motivadores de los riesgos identificados, entendiendo que el proceso pretende determinar situaciones probables, evitando señalar personas a cerca de hechos que están ocurriendo, recuerde que el riesgo tiene que ver con incertidumbre, acerca de algo que en el futuro podría presentarse.

Así entonces, debe revisarse que haya coherencia entre el riesgo, la consecuencia, la causa y la causa raíz.

Riesgo	Causa	Causa raíz	Consecuencia
Qué puede suceder?	*Cómo puede suceder?*	*Por qué ocurre la causa?*	*Qué impactos genera?*

La información relevante de la etapa de identificación de riesgos se registrará inicialmente en el formato de Evaluación, Tratamiento y Monitoreo de riesgos FOPE03, que a su vez retroalimentará la Matriz de Riesgos.

8.2.2 ANÁLISIS DEL RIESGO

En la etapa de análisis se busca asignarle una calificación al riesgo con el objetivo de comprender su magnitud y lograr priorizar los riesgos más importantes.

El riesgo se mide con base en dos criterios: probabilidad e impacto.

8.2.2.1 Probabilidad.

Se entiende por probabilidad el grado en el que es posible que un evento ocurra.

Para determinar la probabilidad, la mesa de expertos o quienes analizan el riesgo, tendrán en cuenta los siguientes criterios:

- La evaluación de la probabilidad no tendrá en cuenta el beneficio de los controles o planes de tratamiento implementados (Se responde a la pregunta ¿Que tan posible es que ocurra el riesgo si no existieran controles o tratamientos de prevención?).
- Seleccionar el nivel de acuerdo a la escala de probabilidad, el analista debe valorar el mayor nivel posible, sea, la posibilidad de que ocurra, la frecuencia de ocurrencia (hechos históricos) y la frecuencia de la actividad que se expone al riesgo.
- El modelo permite que existan calificaciones de varios participantes. En cuyo caso la calificación estará determinada por el promedio de las calificaciones individuales de los analistas que participaron. El promedio de las calificaciones tendrá en cuenta el tipo de participantes; si son de 1ª línea de Defensa, de 2ª línea, de 3ª línea, o del área asesora en riesgos (OAP). Cada grupo tendrá el mismo peso porcentual independiente del número de participantes de cada grupo.

	ESCALA DE PROBABILIDAD				
	NIVEL		**POSIBILIDAD**	**FRECUENCIA OCURRENCIA**	**FRECUENCIA DE LA ACTIVIDAD (punto de riesgo)**
5	Muy Alta	100%	Se espera que el evento ocurra en todas las circunstancias	Más de 1 vez al año.	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.
4	Alta	80%	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año
3	Media	60%	Se espera que ocurra en algunos casos.	Al menos 1 vez en los últimos 2 años.	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año
2	Baja	40%	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
1	Muy Baja	20%	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes)	No se ha presentado en los últimos 5 años.	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año

NOTA: Para determinar el nivel de probabilidad se debe considerar qué tan probable es que ocurra el riesgo si no existieran los controles actuales (ya que el efecto de los controles sobre el riesgo será calificado en la etapa de valoración).

Otras fuentes de información para análisis de la probabilidad:

La escala de frecuencia de eventos se refiere al número de veces que el riesgo se ha materializado en un periodo de tiempo, lo que demanda que la entidad administre una base de datos de eventos, y que esta sea alimentada por las dependencias de manera adecuada y pertinente. La suficiencia de datos será relevante para asignar un mejor nivel de probabilidad.

Otra fuente de información para analizar un mayor grado de exposición al riesgo es el nivel de frecuencia de la actividad que está expuesta al riesgo, sin embargo, estos datos, solo se tomarán como fuente de análisis de la mesa de expertos a la hora de decidir el nivel de probabilidad.

La escala de frecuencia de la actividad es insuficiente por si sola para calificar la probabilidad de un riesgo, por cuanto la probabilidad no depende solamente de la actividad o cosa que se expone a el riesgo (o no para todos los casos), la probabilidad de un riesgo estará determinada por la incertidumbre asociada al evento de riesgo y por los factores de riesgo, como sus causas, debilidades o amenazas.

La frecuencia de la actividad no es de aplicación para todos los riesgos, ya que no siempre se puede determinar la frecuencia de la actividad o frecuencia del objeto o cosa que está expuesta a el riesgo, por ejemplo; frente a un riesgo de terremoto, no es fácilmente identificable ni la actividad expuesta ni mucho menos la frecuencia de la actividad.

El análisis del grupo de expertos será conveniente para determinar el nivel de probabilidad que se ajusta al riesgo, sin embargo, ante cualquier diferencia del equipo, prefiérase el nivel de probabilidad mayor dada las escalas anteriores.

8.2.2.2 Impacto

Es la valoración o medida de las consecuencias que se producen por efecto de la materialización del riesgo.

En el formato de evaluación se describirán las consecuencias esperadas las cuales podrán agruparse por lo menos en los siguientes tipos:

- Económica
- Reputacional
- Legal
- Operacional
- Daño Fiscal
- Derechos Fundamentales

Primero se determinará el valor aproximado de la pérdida en caso de materializarse y su valor se compara con la escala económica del impacto.

El grupo de analistas determinará si existe otra estimación mayor en la escala reputacional u operacional (siempre se preferirá el nivel de impacto más alto).

La escala de impacto para el instituto será:

	ESCALA DE IMPACTO				
	NIVEL		ECONÓMICA	REPUTACIONAL	OPERACIONAL
5	CATASTRÓFICO	100%	Mayor o igual a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario.	No se puede cumplir con la misión de la entidad. No hay posibilidad de lograr los objetivos institucionales.
4	MAYOR	80%	Entre 100 y menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel del sector administrativo, nivel departamental o municipal.	La mayoría de los objetivos Institucionales no se pueden cumplir. Interrupción de las operaciones por tiempo prolongado. Perjudica la prestación de los servicios y entrega de productos.
3	MODERADO	60%	Entre 50 y menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Algunos objetivos institucionales se pueden ver comprometidos. Se interrumpen las actividades
2	MENOR	40%	Entre 10 y menor a 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de alta dirección y/o de proveedores.	Afectación menor a la operación, se hacen reprocesos. Algún objetivo pudiera verse comprometido.
1	LEVE	20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	No se observa interrupción de la operación. Implica algún reproceso menor.

Nota 1: Para los riesgos de corrupción se utilizan otros criterios (preguntas) para analizar el impacto. Ver capítulo de riesgos de corrupción.

8.2.2.3 Nivel de Riesgo Inherente

El nivel de riesgo inherente corresponde al producto del valor de la probabilidad por el impacto sin tener en cuenta el beneficio que generan los controles existentes, es decir, la situación del riesgo presente en las actividades que se desarrollan, sin que medien verificaciones, comprobaciones, revisión de estándares, listas de chequeo, o cualquier otro mecanismo de control y tratamiento establecido.

La zona del nivel del riesgo estará determinada por el siguiente mapa de calor y adoptado dentro de apetito de riesgos del instituto acuerdo a la interacción entre la probabilidad y el impacto:

		IMPACTO				
		1	2	3	4	5
		20%	40%	60%	80%	100%
PROBABILIDAD 5	100%	20%	40%	60%	80%	100%
4	80%	16%	32%	48%	64%	80%
3	60%	12%	24%	36%	48%	60%
2	40%	8%	16%	24%	32%	40%
1	20%	4%	8%	12%	16%	20%
		BAJO	MODERADO	ALTO	EXTREMO	

Por ejemplo,
Para un riesgo cuya calificación sea, Probabilidad = Media e Impacto = Moderado, el nivel de riesgo será, “Moderado” (zona de color “Amarillo”), Y el valor corresponderá al producto del % asignado en la probabilidad por el valor de % asignado en el Impacto.

La información del análisis del riesgo, es decir, la calificación de la probabilidad y el impacto, y el nivel del riesgo inherente quedarán registrados en el formato FOPE03 Evaluación, Tratamiento y Monitoreo de Riesgos.

8.2.3 VALORACIÓN

La etapa de valoración del riesgo está comprendida en dos actividades principales, la calificación de los controles, y la valoración del efecto que tienen éstos sobre el riesgo.

8.2.3.1 Calificación de los Controles

“Entiéndase el control como la medida que mantiene o modifica un riesgo. Los controles incluyen, cualquier proceso, política, dispositivo, práctica, condiciones y/o acciones que mantengan y/o

modifiquen un riesgo. Los controles no siempre logran generar el efecto de modificación planificado"[1].

En esta etapa se realiza un inventario de los controles **existentes**, registrando la mayor información posible sobre el control en cuanto a: cuál es el control y cómo se ejecuta.

La información de los controles y sus calificaciones se registrará en el formato "FOPE03 Análisis del Riesgo".

Los controles identificados deben ser diseñados y valorados de acuerdo con sus atributos.

ATRIBUTOS INFORMATIVOS				
DESCRIPCIÓN DEL CONTROL	**RESPONSABLE**	**DOCUMENTACIÓN**	**EVIDENCIA**	**FRECUENCIA**
Control: Tratamiento implementado	Quien ejecuta	Manual, procedimiento, documento o acto administrativo que formaliza el control	Soporte de ejecución del control o tratamiento	• Continua • Aleatoria

ATRIBUTOS DE EFICIENCIA (CALIFICABLES)		
IMPLEMENTACIÓN	**TIPO**	**EFECTO SOBRE EL RIESGO**
• Automático (25%) • Manual (15%)	• Preventivo (25%) • Detectivo (15%) • Correctivo (10%)	• Probabilidad • Impacto • Ambos

Control Automático: Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.

Control Manual: Controles que son ejecutados por una persona, tiene implícito el error humano.

Control Preventivo: Controles que se ejecutan para prevenir la ocurrencia del riesgo. Es decir, antes y para que no se materialice

Control Detectivo: Son tratamientos que facilitan la identificación o presencia de un factor de riesgo (Causa), de una alerta o proximidad del riesgo, o identificar que el riesgo se materializó

Control Correctivo: Controles que se aplican una vez haya ocurrido la materialización del riesgo, con el propósito de reducir alguna área de impacto.

La calificación del control dependerá de la sumatoria del valor asignado a cada atributo de eficiencia; implementación y tipo de control.

Por ejemplo; un control que sea automático (25%) y preventivo (25%), tendrá una calificación de 25% + 25% = 40%

Los controles del riesgo deben estar orientados a disminuir la probabilidad y/o el Impacto. Es decir, acciones orientadas a tratar las causas raíz, las causas principales, las consecuencias y/o el riesgo directamente.

[1] ISO 31000:2018. Definición de control del riesgo

Cuando exista más de un control para el riesgo, por ejemplo, para dos controles; la calificación del control 2 se aplicará al residuo del riesgo que se obtuvo después del control 1 (según aplique a la probabilidad o al impacto).

8.2.3.2 Nivel de Riesgo Residual

El concepto de Riesgo Residual corresponde a la calificación que se hace del riesgo teniendo en cuenta el efecto de los controles existentes. Este proceso es resultado de multiplicar el valor inicial de la probabilidad o del impacto por el valor del control.

Ejemplo; Si la probabilidad inherente es de 60%, y el control 1 haya sido calificado con 40%: La probabilidad residual será igual a = 60% - (60%x40%) = 60% - 24% = 36%.

Cuando exista más de un control para el riesgo, la calificación del control n se aplicará al residuo del valor de la probabilidad y el impacto después del efecto del control n-1.

Para nuestro ejemplo, en caso de que un control 2 tenga un valor de 30% y que afecte también la probabilidad. La probabilidad residual final tendrá un valor = 36% - (36%x30%) = 25,2%.

Recordemos que el valor del riesgo residual será la multiplicación de la probabilidad por el impacto. Y se ubicará en la zona de calor del mapa de riesgos.

8.3 ETAPA 3. TRATAMIENTO.

El plan de tratamiento es el conjunto de acciones que se implementan para lograr llevar el riesgo residual al nivel del apetito de riesgo definido por la entidad o en su defecto al nivel de tolerancia permitido.

La decisión de qué política de tratamiento de riesgo seguir, responde a cómo llevar el riesgo residual a cumplir con el apetito de riesgo.

El tratamiento *como cualquier control del riesgo,* debe estar orientado a acciones para disminuir la probabilidad y/o el Impacto. Es decir, acciones orientadas a tratar las causas raíz, las causas principales, las consecuencias y/o el riesgo directamente.

El plan de tratamiento se documentará en el mismo formato de Evaluación, Tratamiento y monitoreo del riesgo. Los campos mínimos serán, la descripción de la acción de tratamiento, el responsable, los plazo o fechas.

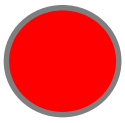
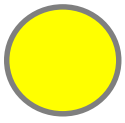
8.3.1 Políticas de tratamiento.

Definir el plan de tratamiento supone que no se acepta el nivel del riesgo residual por cuanto no cumple el apetito o el nivel de tolerancia. Por el contrario, una primera opción es decidir si el nivel de riego residual se puede aceptar o no.

Aceptar un riesgo significa que una vez conocido el nivel de riesgo, se toma la decisión de asumir el riesgo bajo esas condiciones, es decir, que se continuarán con los controles definidos e implementados, pero no se definirá ningún plan de tratamiento. Esta decisión es importante, toda

vez que presume que no es necesario la inclusión de controles adicionales ya que el nivel de riesgo se encuentra en una zona aceptable, se entiende que la Entidad está en la capacidad de gestionar el riesgo residual que se asume.

En el IDU se establecen los siguientes criterios de tratamiento las cuales cumplen con el apetito y tolerancia al riesgo de la entidad:

Nivel de Riesgo residual	DECISIÓN
 EXTREMO	Deben establecerse los mecanismos de control que se implementarán para tratar el riesgo considerando primero las causas que estén desprotegidas y segundo aquellos controles que tienen posibilidad de ser mejorados. Las acciones deben orientarse a mejorar los controles actuales o la inclusión de nuevos controles o mecanismos de tratamiento del riesgo.
 ALTO	No cumple el apetito de riesgos ni el nivel de tolerancia: Es obligatorio definir e implementar un plan de tratamiento que trate el riesgo y como resultado de éste el nivel de riesgo residual disminuya a nivel Moderado o Bajo
 MODERADO	No cumple el apetito de riesgo, pero si con el nivel de tolerancia: Se recomienda la definición de un plan de tratamiento (aunque no es obligatorio).
 BAJO	Cumple con el apetito de riesgo: Se asumen el riesgo residual. No requiere plan de tratamiento. Se Continúa con los controles y mecanismos de tratamiento existentes.

NOTA: Todos los riesgos de corrupción deben llevar acciones de tratamiento.

Las 3 políticas de tratamiento, están definidas así:

POLÍTICA DE TRATAMIENTO	DESCRIPCIÓN
Evitar	Es eliminar el riesgo. Implementar un plan de tratamiento para que no exista la probabilidad de estar expuestos a ese riesgo. (Generalmente se elimina la actividad o cosa que está expuesta al riesgo). El riesgo no hace parte de los tipos de riesgos contemplados dentro del Apetito de Riesgo de la Entidad, o su nivel de riesgo residual no puede reducirse y por lo mismo no satisface el nivel de Tolerancia al riesgo del Instituto.
Reducir	Esta política, demanda que se implemente un plan de tratamiento (Controles) que logre disminuir la Probabilidad de que el riesgo se presente, y/o disminuir el Impacto que ocasiona el riesgo en caso de materializarse. El plan de tratamiento debe lograr que el nivel de riesgo residual se reduzca hasta que cumpla el Apetito de riesgo o en su defecto el Nivel de Tolerancia al riesgo del Instituto.
Aceptar	Se asume el riesgo bajo las condiciones actuales ya que satisface el apetito de riesgo de la entidad. Se decide continuar con los controles existentes, sin incurrir en tratamientos adicionales.

8.4 ETAPA 4. MONITOREO Y SEGUIMIENTO

Es necesario para el IDU distinguir el seguimiento del monitoreo, la diferencia principal es que el monitoreo se enmarca en la revisión completa y exhaustiva de toda la información asociada al riesgo; desde su contexto hasta las acciones de tratamiento, el monitoreo se realiza de forma anual, presentando para cada vigencia toda la información de los riesgos actualizada.

El seguimiento se realiza de forma cuatrimestral, enfocado principalmente en el análisis de los indicadores del riesgo y el reporte de eventos de riesgos ocurridos. Sin embargo, el seguimiento podría incluir modificaciones a cualquier característica del riesgo si se requiere

El monitoreo es la fase de la Administración del Riesgo en la cual se efectúan las verificaciones al sistema en todas sus dimensiones, corresponde a la rutina mediante la cual se vigila el comportamiento y se determinan los cambios relevantes en cada uno de los componentes de la administración del riesgo y las oportunidades.

El monitoreo de riesgos y oportunidades es una actividad continua, en el cual se deben tener en cuenta los cambios que se presentan en el contexto, en la estructura, los procesos o en los criterios para la toma de decisiones que puedan hacer que el análisis de riesgos y oportunidades varíe con respecto a la situación actual.

Adicionalmente, el monitoreo y los seguimientos incluyen la verificación del cumplimiento del plan de tratamiento del riesgo.

En el monitoreo, se debe verificar la implementación de los controles definidos en el plan de tratamientos. Es decir, una vez implementado el tratamiento del riesgo, se debe actualizar la evaluación de los controles y determinar el efecto que tiene sobre el riesgo.

Es posible que la iniciativa de revisión y actualización del riesgo monitoreo se presente por solicitud de una auditoría interna o externa, o por solicitud de la segunda, tercera línea de defensa o la línea estratégica. Para lo cual el encargado del proceso debe disponer lo necesario para la realización oportuna del monitoreo. De todas formas, es adecuado para el IDU que mínimo en el plazo de un año se haya realizado un ejercicio de monitoreo completo en el que se haya revisado toda la información del riesgo.

La información del monitoreo a los riesgos se registrará en el mismo formato de Evaluación, Tratamiento y monitoreo del riesgo.

8.5 COMUNICACIÓN Y CONSULTA

Son actividades continuas que la Entidad lleva a cabo para suministrar, compartir y obtener información con las partes interesadas respecto a la información del riesgo. Es un proceso continuo que tiene lugar en todas las etapas de la administración del riesgo.

La consulta es un proceso de doble vía de la comunicación informada entre la Entidad y sus partes involucradas, acerca de algún tema en relación con el riesgo, antes de tomar una decisión o determinar una dirección para dicho tema.

La información del riesgo deberá presentarse en los medios de divulgación internos vigentes en la entidad, o cuando la normatividad así lo requiera se hará una publicación en otro medio de carácter

externo. De todas formas, la información del riesgo de los procesos se consolidará por la Oficina Asesora de Planeación y se publicará en el Mapa de procesos.

La matriz de riesgos del proceso y la matriz de riesgos de corrupción deberán ser enviados a la OAP para consolidación por medio del Sistema de información de Correspondencia vigente.

Para los riesgos de corrupción, las matrices se publicarán en la página WEB de la entidad en el enlace del "Plan Anticorrupción" o el que le reemplace.

Los demás documentos de trabajo, como actas de reunión, listas de asistencia a sensibilizaciones deberán ser controladas por la dependencia dueña del riesgo.

8.6 GESTIÓN DE EVENTOS DE RIESGOS MATERIALIZADOS (ERM)

Entiéndase como evento de riesgo materializado, la ocurrencia de un incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado y que puede afectar el objetivo del proceso.

La gestión frente a un evento de riesgo incluye tres momentos importantes:

- Previo. Cuando aún no ha pasado. Contemplamos los posibles eventos y planeamos las acciones para atender el evento en caso de ocurrencia.
- Durante: El segundo tiene que ver con la atención del evento presentado, cuyo objetivo es detener o disminuir las pérdidas o efectos ocasionados. Incluye la comunicación a partes interesadas.
- Posterior: el tercero momento, es la definición e implementación de las acciones correctivas que tratan las causas que ocasionaron el evento con el propósito de reducir la probabilidad de volverse a presentar y/o reducir el valor del impacto del riesgo.

Previo:

Durante las fases de identificación y monitoreo de riesgos, las áreas líderes del proceso identificarán y mantendrán actualizadas la información de las acciones de repuesta y/o contingencia que se deberían ejecutar en caso de un evento de riesgo materializado. Dichas acciones serán registradas en el formato FOPE06 Matriz de Riesgos.

Las acciones de respuesta y/o contingencia son todas aquellas actividades que se proyectan ejecutar para atender el evento inmediato, puede incluir procedimientos específicos de contingencia o recuperación y acciones de comunicación y gestión con grupos de interés (ciudadanos, entes de control u otras entidades).

El líder del proceso debería en los seguimientos periódicos verificar que la información planificada sobre las acciones de respuesta permanece actualizada.

Durante:

Atender el evento presentado es lo más importante en la gestión de un riesgo materializado. Su objetivo es detener o disminuir las pérdidas o efectos ocasionados. Se debe tener en cuenta:

- Revisar las acciones que se consideraron realizar frente a la ocurrencia del evento.
- Activar los planes de contingencia si los hubiere.
- Comunicar a las personas que deban atender el evento.
- La atención del evento debe orientarse a detener o evitar la propagación del daño o perdida.
- Comunicar a las autoridades o entidades externas que requieran conocer los hechos por posibles hechos de corrupción o porque pueden ser afectadas por el evento presentado.

Posterior:

En este momento se definen e implementan las acciones correctivas que tratan las **causas** que ocasionaron el evento ocurrido, con el propósito de que no se vuelva a presentar o reducir su probabilidad de ocurrencia. Las acciones también pueden incluir acciones para reducir el impacto de futuras pérdidas, en especial cuando el riesgo es de carácter externo.

Las acciones pueden incluir la revisión del riesgo y si es el caso el ajuste a la información del riesgo o de cualquier característica (causas, controles, probabilidad o impacto entre otros).

8.6.1 Reporte de Eventos de riesgos materializados:

El reporte de un evento de riesgo materializado deberá realizarse junto con los seguimientos periódicos que se realizan a los riesgos (o antes si así lo considera el líder del proceso), allí se registra el evento y el plan de acción que incluye las correcciones y acciones correctivas.

La información se registrará en el formato FOPE03 de Evaluación, Tratamiento y Monitoreo de riesgos.

Los eventos relacionados con accidentes laborales no se registrarán inicialmente en la matriz de riesgos FOPE06, ya que seguirán lo definido en el Subsistema de Seguridad y Salud en el trabajo, específicamente lo requerido en el procedimiento PRAC12 de incidentes y accidentes.

La OAP consolidará en una sola base de datos los eventos de riesgos ocurridos que se le informen, y presentará de forma anual las estadísticas junto al informe anual de la política de riesgos.

8.7 GESTIÓN DE OPORTUNIDADES

Entiéndase como **Oportunidad** (del latín Opportunitas) a lo conveniente de un contexto y a la confluencia de un espacio y un periodo temporal apropiado para obtener un provecho o cumplir un Objetivo."[2].

Como beneficio de implementar un sistema de gestión de la calidad la Entidad debería tener la capacidad de abordar los riesgos y gestionar las oportunidades asociadas a su contexto para facilitar el cumplimiento de sus objetivos. La gestión de riesgos no solo procura la minimización de los efectos negativos, sino que debiera identificar y maximizar las oportunidades a medida que surjan. (ISO9001:2015).

[2] https://definicion.de/oportunidad

8.7.1 Identificación de oportunidades.

Una vez identificado el contexto estratégico, podemos conocer la información relevante a los factores negativos y positivos que están influenciado la gestión. Por un lado, se estima conveniente que los factores negativos sean gestionados por la gestión de riesgos y/o planes de mejoramiento que correspondan, y por el otro, que los factores positivos sean analizados, priorizados y tratados siguiendo los lineamientos que aquí se desarrollan en cuanto a la gestión de oportunidades.

Así entonces, la primera fuente de información son los factores analizados en el componente de Oportunidades del DOFA identificados en el Contexto Estratégico.

Las oportunidades allí registradas deberán estar relacionadas en el formato "Matriz de Oportunidades", el propósito es que el instrumento facilite el análisis y la valoración de las oportunidades, se registre la decisión de aprovechamiento y contribuya al seguimiento de las estrategias. Adicional el grupo de análisis podrá incluir nuevas oportunidades para ser analizadas.

8.7.2 Análisis y Valoración de oportunidades.

El análisis de las oportunidades dará como resultado una priorización de estas, entregando información para decidir qué hacer con dicha oportunidad. Para el análisis, se calificará la oportunidad considerando la probabilidad de ocurrencia y el impacto que la oportunidad puede generar.

Criterios para Calificación de la Probabilidad.

Escala de Probabilidad de Oportunidades

Nivel		Descripción
5	Casi segura	Se espera que la oportunidad siempre se presente para el contexto en el que se desarrolla la actividad.
4	Alta	Se espera que la oportunidad se materialice en la mayoría de las circunstancias.
3	Posible	Es posible que suceda, se espera que ocurra en algunos casos.
2	Baja	Probabilidad de ocurrencia baja, la oportunidad puede ocurrir en algún momento.
1	Remota	Aunque existe la probabilidad, la oportunidad podría ocurrir solo en circunstancias excepcionales (poco comunes).

Criterios para Calificación de Impacto.

Escala de Impacto de Oportunidades

Nivel		Descripción
5	Exitoso	Los beneficios de aprovechar la oportunidad son evidentes en la mayoría de las áreas de gestión o impacto.
4	Mayor	Se observan beneficios del alto impacto en algunas de las áreas de gestión. La relación costo-beneficio es eficiente para el Instituto.
3	Moderado	Beneficios moderados en algunas de las áreas de gestión. La relación costo-beneficio está equilibrada
2	Menor	Beneficios poco relevantes para las áreas de gestión. Demanda un esfuerzo que poco compensa la relación costo-beneficio. Es fácil perder los efectos de su implementación o aprovechamiento.
1	Insignificante	No se perciben beneficios evidentes por el aprovechamiento de la oportunidad

Factores de impacto:

Ciudadanía, Otros grupos de interés, Productos/servicios, Objetivos, Financiera, Imagen, Requisitos Legales (incluye contractuales y propios), Operacional/Organizacional, Personal, Información, Ambiental.

Así entonces, cada área de impacto tendrá una calificación con un valor entre 1 a 5, y el nivel de impacto de toda la oportunidad será el promedio aritmético de los resultados de todos los factores.

Nivel de Oportunidad:

El nivel total de la Oportunidad será el Producto de su Probabilidad por el nivel de Impacto.
El nivel de oportunidad es un índice que nos permite priorizar las oportunidades considerando el valor esperado de la materialización de la oportunidad. Con respecto a este nivel, se decidirá la política de tratamiento para la oportunidad.

Los valores posibles de una oportunidad están indicados por el siguiente mapa:

MAPA DE OPORTUNIDADES

			IMPACTO				
			1	2	3	4	5
			Leve	**Menor**	**Moderado**	**Alto**	**Mayor**
PROBABILIDAD	5	**Muy Alta**	5 MONITOREAR	10 MONITOREAR	15 MONITOREAR	20 APROVECHAR	25 APROVECHAR
	4	**Alta**	4 OMITIR	8 MONITOREAR	12 MONITOREAR	16 APROVECHAR	20 APROVECHAR
	3	**Media**	3 OMITIR	6 MONITOREAR	9 MONITOREAR	12 MONITOREAR	15 MONITOREAR
	2	**Baja**	2 OMITIR	4 OMITIR	6 MONITOREAR	8 MONITOREAR	10 MONITOREAR
	1	**Muy Baja**	1 OMITIR	2 OMITIR	3 OMITIR	4 OMITIR	5 MONITOREAR

8.7.3 Tratamiento de la oportunidad.

Según se mostró en el mapa de oportunidades anterior, de acuerdo con el nivel de la oportunidad se recomiendan los siguientes criterios de tratamiento:

NIVEL	POLÍTICA	DESCRIPCIÓN
16 – 25	APROVECHAR	En este nivel de oportunidad, la expectativa son los beneficios importantes que tienen un alto grado de que se hagan realidad. En esta situación, se deberías abordar la oportunidad y determinar la estrategia y las acciones a seguir para **aprovechar** y capitalizar los beneficios esperados.

5 – 15	MONITOREAR	La oportunidad se encuentra en un estado intermedio, es decir que, aunque existen beneficios que podrían percibirse, aun las condiciones y probabilidades podrían no ser las más convenientes, por lo que no se recomienda iniciar una estrategia o acción para implementar o capitalizar dicha oportunidad. Sin embargo, dada la combinación que expone la oportunidad, se recomienda que se monitoree dicha oportunidad en el siguiente periodo de análisis y se revise si ha mejorado su nivel de probabilidad y/o sus posibles impactos positivos, para decidir si se inician con las estrategias para su aprovechamiento y capitalización. En todo caso, el líder del proceso podrá considerar la implementación de una estrategia para este nivel sin esperar al siguiente periodo de análisis.
1 – 4	OMITIR	En este nivel se recomienda que la oportunidad se descarte, y que no se inicien acciones para su aprovechamiento, se entiende que la relación costo-beneficio no es conveniente para el Instituto. La decisión de no hacer nada frente a la oportunidad, sería conveniente en el sentido de que no compensa el esfuerzo frente a las bajas posibilidades de que se materialicen los pocos beneficios esperados.

La estrategia deberá definirse en términos de las acciones que se ejecutarán con el propósito de aprovechar la Oportunidad. En la matriz de oportunidades se definirá las actividades, responsables, fechas y estado de avance, en algunos casos será necesario la referencia a programas, planes o proyectos a implementar en el marco de la estrategia para aprovechar la oportunidad.

8.8 CONSIDERACIONES PARTICULARES SEGÚN EL TIPO DE RIESGO

8.8.1 Riesgo de corrupción.

La metodología para la gestión del riesgo de corrupción (aunque su enfoque sigue el marco general de las etapas de administración del riesgo expuestas en el presente manual), seguirá lo establecido en el documento “Guía para la Administración de Riesgos para entidades públicas” del DAFP y su adecuación a los requisitos propios del IDU.

Entiéndase por riesgo de corrupción la “Posibilidad de que por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado”[3].

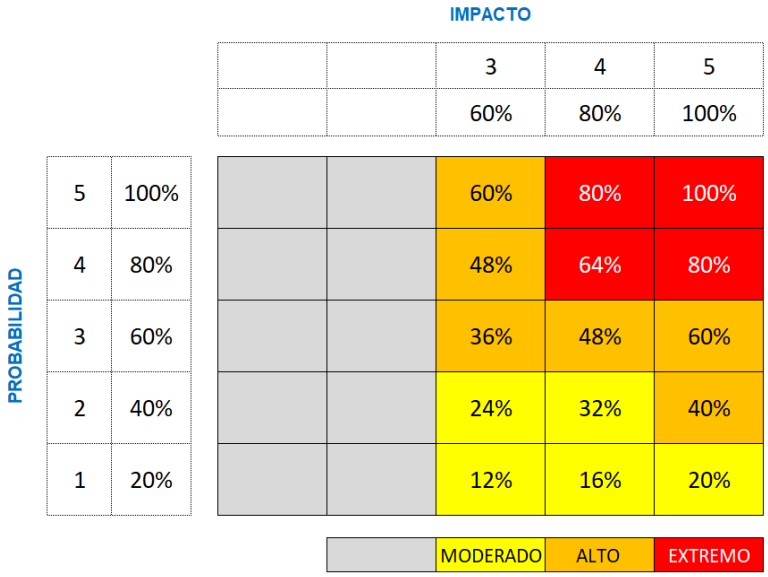
El instrumento definido en el IDU para registrar la información del riesgo de corrupción es el Formato FOPE10 Evaluación, Tratamiento y Monitoreo del Riesgo de Corrupción el cual alimenta la Matriz de Riesgos de Corrupción FOPE05.

El seguimiento para los riesgos de corrupción deberá realizarse de forma cuatrimestral, o diferente si la normatividad así lo específica.

El mapa de riesgos de corrupción será el siguiente

Mapa de riesgos de Corrupción

[3] Guía para la Administración de los riesgos de gestión, corrupción y seguridad digital y el diseño de controles en entidades públicas. Agosto de 2018. DAFP



De acuerdo con el requisito normativos, se restringe el uso de los dos primeros niveles del impacto para el riesgo de corrupción. El nivel de riesgo estará comprendido en nivel moderado, alto y extremo.

Así mismo, no se debe aceptar el riego de corrupción, por lo que independiente del nivel de riesgo residual, siempre deberá definirse un plan de tratamiento del riesgo.

Las matrices de riesgos deberán ser publicados en la página WEB del IDU.

Para la administración del riesgo de corrupción deberá seguirse anualmente lo programado en el Plan Anticorrupción y de Atención al Ciudadano del Instituto.

Para los **riesgos de soborno** se seguirán los lineamientos e instrumentos que se definan en el marco de la del Subsistema de Gestión Antisoborno, toda vez que es una decisión de mejora del Instituto adicional a los requisitos exigidos por la normatividad vigente en materia de riesgos de corrupción.

ANALISIS DE CAUSAS:

Dentro de las posibles causas que deban ser analizadas para los riesgos de corrupción, se recomienda la siguiente lista, (pero no limitarse solamente a éstas):

1. Procesos que involucran trámites que implican manejo de dinero en efectivo.
2. Discrecionalidad para la gestión de trámites y servicios (sin protocolos o procedimientos de atención).
3. Falta de segregación de funciones por restricciones de planta.
4. Discrecionalidad para la toma de decisiones en grupos restringidos de servidores.
5. Servidores con conflictos de interés en los temas sobre los cuales pueden incidir con su toma de decisiones.
6. Ausencia o debilidad de medidas y/o políticas para la identificación y manejo de conflictos de interés.

7. Fallas en el apoyo jurídico interno que generan interpretación subjetiva de las normas o reglamentos.
8. Ausencia de publicación de los procesos precontractuales, contractuales o pos contractuales en Secop.
9. Factores externos de presión en temas regulados que pueden incidir en las decisiones institucionales.
10. Fases de análisis de los requisitos con excesiva reserva que impida la transparencia en determinado proceso.
11. Gestión Documental con fondos acumulados que no garantizan los registros y memoria institucional
12. Inexistencia de archivos contables.
13. Arqueos de caja adelantados por personal no idóneo y sin la autoridad requerida (adelantada por el mismo servidor o bien por otro servidor que no cuenta con un nivel jerárquico superior).
14. Falta de inclusión de acuerdos de confidencialidad y manejo de información interna que facilita su divulgación y uso no autorizado de información privilegiada.
15. Ausencia de sistemas de información, que pueden facilitar el acceso a información y su posible manipulación o adulteración.
16. Falta de herramientas tecnológicas para la transmisión de datos e información entre procesos y a nivel externo.

8.8.2 Riesgo de seguridad de la información (SI).

El concepto de seguridad de la información abarca el concepto de seguridad digital, es así que, en el IDU, los riesgos de seguridad de la información (SI) contemplan los riesgos de seguridad digital. Para la gestión de riesgos asociados a la seguridad de la información se seguirán las etapas de administración del riesgo definidas en el presente manual, teniendo en cuenta las siguientes consideraciones particulares:

- Los riesgos de SI se registrarán en el formato FOPE19 ¨Matriz de Riesgos de Seguridad de la Información¨.

- Cada riesgo de SI deberá tener asignado el Dueño del riesgo.

    - ¿Quién es el Dueño del riesgo?:
      Es el propietario o responsable del riesgo, es decir, la persona a la que se le ha dado la autoridad para valorar y tratar un riesgo en particular. El dueño de riesgo para el caso de SI tendrá directa relación con el Activo de Información. Por ejemplo, en el IDU, el dueño de un riesgo asociado a la información de la nómina donde participan diferentes actores como, el Profesional de nómina, el Profesional Coordinador del grupo de nómina, el Subdirector Técnico de Talento Humano, el Director Técnico Administrativo o el Subdirector General de Gestión Corporativa, la recomendación es que se prefiera como dueño del riesgo al gerente o líder de la línea operativa que gestiona directamente el activo, para nuestro ejemplo, se recomienda que el Subdirector Técnico de Talento Humano sea el dueño del riesgo asociado a la información de la nómina. En todo caso, los líderes de proceso definirán está asignación, considerando siempre las responsabilidades y funciones aplicables al

Instituto y a las recomendaciones de la 2ª línea de defensa frente a este tipo de riesgo (SGGC – STRT).

- Deberá dejarse evidencia de la aceptación por parte del Dueño de los riesgos asignados, y de su nivel de riesgo residual. Esta aprobación se realizará cuando se identifica por primera vez el riesgo, y por lo menos una vez de forma anual cuando se realice la calificación del riesgo.
- La STRT propondrá el documento para la aprobación del riesgo por parte de los Dueños, el cual contendrá como mínimo la lista de riesgos donde se registre el código del riesgo, la descripción, el nivel de riesgo inherente y el nivel de riesgo residual.

- Los riesgos de SI se identifican por grupos de activos de información; grupos previamente identificados por la STRT y asociados a los procesos de la Entidad.

- La descripción el riesgo de SI es el agrupamiento de la información contenida en el formato FOPE19 en los campos: activo de información, tipo de riesgo, amenazas y vulnerabilidades del riesgo.

- Los tipos de riesgo de SI son tres:
  - C: Pérdida de Confidencialidad
  - I: Pérdida de Integridad
  - D: Pérdida de Disponibilidad

  Un riesgo de SI puede estar asociado a uno o más tipos de riesgo.

- Cada riesgo debe contemplar las amenazas potenciales que lo afectan, y para cada amenaza deberán identificarse las vulnerabilidades asociadas.

- La amenaza es la causa potencial de un incidente no deseado, que puede resultar en un daño al activo de información.

- La vulnerabilidad es entendida como la debilidad que permite o facilita la ocurrencia de la amenaza.

- El nivel del riesgo dependerá del producto de la probabilidad y el impacto, conforme a los criterios definidos en la etapa de análisis del riesgo. La calificación del riesgo se registrará inicialmente en el formato definido para el Análisis del Riesgo

- Los mecanismos de control o tratamiento frente a los riesgos se definirán como salvaguardas y su identificación y calificación seguirán los criterios definidos en la etapa de valoración del riesgo.

- Para cada riesgo de SI se deben incluir los controles del Anexo A de la norma ISO 27001 y que sean aplicables en el IDU.

- La coordinación y asesoramiento para la administración del riesgo de SI será responsabilidad de las dependencias líderes del Subsistema de Gestión de Seguridad de la Información: La Subdirección General de Gestión Corporativa y la Subdirección Técnica de Recursos Tecnológicos.

- Como los procesos contienen tipos de activos de información similar, por ejemplo, en todos hay activos como equipos de cómputo, carpetas y documentos, entonces; existen riesgos que pueden aplicar a todos o a un grupo de procesos. Por tal motivo, los riesgos que se identifiquen serán de tipo transversal, para lo cual la STRT junto con el proceso o las áreas lideres realizarán el análisis de los riesgos respectivos y serán de aplicación al proceso o grupo de procesos que les apliquen dichos riesgos.

- La OAP realizará un acompañamiento y asesoramiento en cada una de las etapas de la administración de riesgos, en los aspectos metodológicos.

8.8.3 Riesgos contractuales (matriz anexa al Contrato).

La gestión de los riesgos asociados al proceso de contratación se hará de acuerdo con el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación expedido por Colombia Compra Eficiente, teniendo en cuenta las siguientes condiciones particulares para el IDU.

- La matriz de riesgos del IDU (FOGC01) contiene los riesgos generales que pueden presentarse en las diferentes etapas del proceso contractual, desde su planificación, selección, ejecución y liquidación.

- Los riesgos específicos a un proceso de contratación particular deberán ser identificados por las áreas encargadas de presentar los insumos para la etapa de selección, estas áreas deberán incluir la Matriz de Riesgos en los Estudios Previos del Proceso de Contratación, y reflejarse en los pliegos de condiciones o su equivalente y en la minuta del contrato. Es de aclarar que las áreas encargadas de la inclusión de la matriz de riesgos recibirán el acompañamiento respectivo cuando así lo requieran de las áreas que consideren tanto técnicas (asociadas al objeto del contrato) como de asesoría en el tema de gestión de riesgos.

- El seguimiento y monitoreo a los riesgos contractuales corresponde a cada área dependiendo de la etapa en la que se encuentre el contrato. Así, por ejemplo, si se encuentra en la etapa de Ejecución Contractual, y su objeto corresponde a la ejecución de una obra, le corresponderá a la dependencia que ejerce la supervisión y coordinación del contrato en esa etapa. Para el seguimiento a los riesgos contractuales se usará la hoja de seguimiento En el mismo archivo de la Matriz de Riesgos. El seguimiento a los riesgos deberá incluir la participación de las instancias que tenga el riesgo asignado (contratista, interventoría, supervisión).

- Riesgos en contratación: Las matrices debidamente aprobadas deberán ser documentos anexos al correspondiente contrato. Es decir, que su archivo y publicación se rige por lo definido en la gestión contractual.

9 REFERENCIAS BIBLIOGRÁFICAS

- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Bogotá, D.C., (2022). Sexta Versión.

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del Riesgo, Principios y Directrices. NTC-ISO 31000. Bogotá D.C., 2011. (esta norma es una adopción idéntica por traducción de la norma ISO 31000:2009).

- COLOMBIA COMPRA EFICIENTE. Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación. Bogotá D.C., 2013.