Control de Cambios		
Versión	**Fecha**	**Descripción de la Modificación**
1	21/07/2008	Creación de la Guía
2	05/10/2009	Actualización de acuerdo a lineamientos del Departamento Administrativo de la Función Pública
3	13/01/2012	Inclusión de elementos referentes al contexto estratégico y Mapa de Riesgos Institucional
4	10/12/2013	Actualización de Guía por inclusión de elementos de la estrategia anticorrupción
5	12/06/2015	Actualización de la guía por ajuste institucional
6	31/07/2017	Se realiza actualización de la guía por definición de nuevos criterios para la valoración del riesgo
7	26/11/2018	Se incluye lineamientos de la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades públicas
8	03/01/2019	Se tiene en cuenta observaciones del comité institucional de control interno, se especifica la identificación de riesgos, valoración de riesgos, se incluye monitoreo de riesgos y plan de gestión de riesgos
9	28/01/2020	Se incluye la revisión de los objetivos estratégicos y de proceso por parte de la Oficina Asesora de Planeación. La fase de monitoreo y revisión de los riesgos cambia la periodicidad de desarrollo. Se incluye los pasos de solidez individual de controles, solidez conjunta de controles, apetito al riesgo y tolerancia al riesgo. Se incluyen las categorías de tratamiento de riesgo
10	12/08/2020	Se actualizo el formato cambiándolo de proceso, se ajustó como una guía, se actualizó el formato anexo
11	14/07/2022	Se actualiza la metodología en elementos relacionados con la identificación y valoración del riesgo tomando como base la Guía para la administración del riesgo y el diseño de controles en Entidades públicas, versión 5 de diciembre de 2020, emitida por el Departamento Administrativo de la Función Pública. Se ajusta la guía con la incorporación de los riesgos de fuga de capital intelectual, corrupción en trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo.

Elaboró	Revisó	Aprobó
Viviana Galeano Contratista Oficina Asesora de Planeación	Iván Ernesto Rojas Jefe Oficina Asesora de Planeación	Comité Institucional de Coordinación de Control Interno

Tabla de contenido

1. Objetivo

Establecer una metodología integral para la Administración del Riesgo en el Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER en cada una de las etapas de gestión de acuerdo a la normatividad vigente.

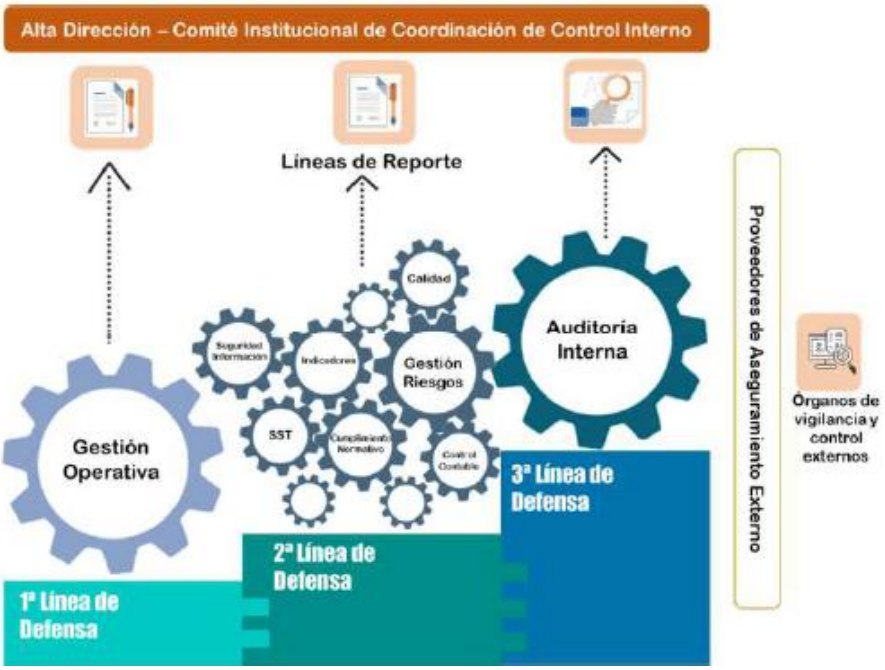
2. Alcance

La presente guía aplica a todos los procesos y niveles del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER y a todas las actividades ejecutadas por los servidores públicos, contratistas y proveedores dentro de la operación de dichos procesos, desde la identificación y valoración hasta el tratamiento de los riesgos estratégicos, de gestión, corrupción, seguridad de la información, fuga de capital intelectual, de corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo.

3. Responsables

El Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER define su estrategia de aplicación y los roles y responsabilidades frente a los riesgos identificados, los cuales se precisan a partir de las líneas de defensa establecidas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG – Versión 4.

Figura No. 1 Líneas de defensa para la Administración del Riesgo



Fuente: Manual Operativo MIPG, V4, 2020

La siguiente tabla detalla cada una de las responsabilidades frente a la gestión del riesgo de las líneas de defensa del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER:

Tabla No. 1 Roles y responsabilidades

Línea de defensa	Responsables	Responsabilidad frente a la gestión del riesgo
Línea estratégica	Alta Dirección - Comité Institucional de Coordinación de Control Interno	1. Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento. 2. Aprobar los niveles de aceptación del riesgo (capacidad, tolerancia y apetito del riesgo). 3. Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. 4. Analizar los riesgos, vulnerabilidades, amenazas que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad, gestión de los procesos y capacidades para prestar servicios. 5. Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del Plan Estratégico Institucional.
Primera línea de defensa	Líderes de Procesos Responsables de proyecto Servidores en general	1. Identificar, valorar, evaluar y actualizar cuando se requiera los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a los procesos. 2. Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. 3. Ejecutar y supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. 4. Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. 5. Definir y ejecutar los planes o acciones para la mitigación de riesgos, de acuerdo a los niveles de riesgo residual definidos en el marco referencia para la gestión del riesgo. 6. Definir y hacer seguimiento a los niveles de aceptación del riesgo (capacidad, tolerancia y apetito del riesgo).
Segunda línea de defensa	Oficina Asesora de Planeación	1. Asesorar a la línea estratégica en el análisis del contexto interno y externo, la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. 2. Capacitar al grupo de trabajo de cada dependencia en la herramienta para la gestión del riesgo. 3. Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. 4. Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. 5. Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad. 6. Revisar que el cargue de información en la herramienta para la gestión del riesgo esté acorde con lo aprobado por el líder del proceso. 7. Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. 8. Socializar y publicar el mapa de riesgos institucional. 9. Presentar al Comité Institucional de Coordinación de Control Interno el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos. 10. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. 11. Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. 12. Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. 13. Revisar los planes o acciones establecidos para cada uno de los riesgos identificados, con el fin de que se tomen medidas oportunas y eficaces. 14. Efectuar de forma periódica el monitoreo a los niveles de aceptación del riesgo (capacidad, tolerancia y apetito del riesgo).
Tercera línea de defensa	Oficina de Control Interno	1. Evaluar la efectividad de la administración de los riesgos en la entidad, incluida la pertinencia y efectividad de los controles 2. Presentar al Comité de Coordinación de Control Interno cualquier cambio o impacto identificado en la evaluación del riesgo. 3. Ejercer su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación para garantizar el cumplimento efectivo de los objetivos. 4. Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

Fuente: Elaboración propia con base en el Manual Operativo MIPG, V4, 2020 (Dimensión 7) y la Guía rol de las Oficinas de Control, 2018

4. Definiciones

Para la administración del riesgo en el Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, se tendrán en cuenta las siguientes definiciones:

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

  Nota: Los eventos potenciales hacen referencia a la 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 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 de Corrupción:** posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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

- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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

- **Riesgo Inherente:** nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

- **Riesgo Residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.

- **Control:** medida que permite reducir o mitigar un riesgo.

- **Causa Inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz:** causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Factores de Riesgo:** son las fuentes generadoras de riesgos.

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

- **Integridad:** propiedad de exactitud y completitud.

- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.

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

- **Activo:** 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.

- **Nivel de riesgo:** es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Tolerancia del riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la entidad.

- **Comité Institucional de Coordinación de Control Interno:** es el órgano asesor e instancia decisoria en los asuntos de control interno de una entidad pública (Decreto 1083 de 2017, artículo 2.2.21.1.5).

- **Comité Institucional de Gestión y Desempeño:** es la instancia encargada de orientar, articular y ejecutar las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y Gestión – MIPG.

- **Trámite:** conjunto de requisitos, pasos, o acciones reguladas por el Estado dentro de un proceso misional que deben efectuar los ciudadanos, usuarios o grupos de interés ante una entidad u organismo de la administración pública o particular que ejerce funciones administrativas, para acceder a un derecho, ejercer una actividad o cumplir con una obligación prevista o autorizada por la ley.

- **OPA:** conjunto de requisitos, pasos o acciones dentro de un proceso misional que determina una entidad u organismo de la administración pública, o particular que ejerce funciones administrativas, para permitir el acceso de los ciudadanos, usuarios o grupos de interés a los beneficios derivados de programas o estrategias cuya creación, adopción e implementación es potestativa de la entidad.

- **Lavado de activos:** el Lavado de Activos es un delito, que consiste en dar una apariencia de origen legítimo o lícito a bienes - dinerarios o no, que en realidad son productos o "ganancias" de delitos graves como: Tráfico ilícito de drogas, Trata de Personas, Corrupción, secuestros y otros (UNODC, 2021).

- **Financiación del terrorismo:** la Financiación del Terrorismo está relacionada con los fondos, bienes o recursos a los que acceden las organizaciones terroristas o los terroristas para poder costear sus actividades (UIAF, 2013).

5. Condiciones generales

- La presente guía corresponde a la Política de Administración del Riesgo adoptada en el Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER.

- La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad.

- Para los riesgos de corrupción, de corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo, no se admite aceptación del riesgo.

- La determinación de los valores de la capacidad, tolerancia y apetito de cada riesgo es definida por cada proceso, y es aprobada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno.

- La identificación de riesgos debe realizarse por lo menos una vez al año por los responsables de cada proceso junto con su equipo de trabajo, a partir del contexto general de la entidad, y del análisis de los objetivos estratégicos y de gestión de cada proceso.

- En complemento con el aspecto anterior, la identificación de riesgos se debe realizar, en otros momentos diferentes de la anualidad así:

*Cuando se materializa un riesgo, es necesario que se evalúe su estructura y controles para determinar si continua o debe ajustarse.

*Cuando en el ejercicio de las funciones, planes, programas, proyectos, procesos, procedimientos etc., o por cambios en el contexto (interno y externo) el responsable del proceso identifique que es necesario gestionar nuevos riesgos.

*Por resultados de las auditorías internas o informes de ley o seguimiento de la Oficina de Control Interno o por los resultados de los informes de auditoría de los entes de control externos.

- Se ha dispuesto como anexo a la presente guía, una herramienta en formato Excel, para la gestión de los riesgos definidos en la entidad.

- Los responsables de cada proceso, antes del 15 de enero de cada vigencia, deben enviar su mapa de riesgos a la Oficina Asesora de Planeación para su revisión, consolidación y publicación, la cual se debe realizar a más tardar el 31 de enero de cada año.

- Es responsabilidad de los líderes de proceso la socialización de los resultados obtenidos entre los miembros de su equipo y es responsabilidad de cada servidor público y contratista del IDIGER consultar permanentemente los riesgos documentados a fin de tener conocimiento de las situaciones de riesgo existentes.

- El consolidado de los mapas de riesgo debe publicarse en la página web de la entidad. La oficina Asesora de Planeación consolida la información entregada por los procesos, y la Oficina de TIC´s publica el Mapa de Riesgos Institucional en la página web en el link de transparencia (Numeral 4.3.1 Planes institucionales y estratégicos) para conocimiento de la ciudadanía e internamente por correo electrónico se socializará la actualización del mapa de riesgos a servidores públicos y contratistas del IDIGER.

- Cada proceso debe garantizar la ejecución de los controles establecidos para los riesgos contemplados en cada vigencia.

- Cuando el equipo responsable del proceso, producto del seguimiento y la revisión quisiera ajustar la redacción de un riesgo, incluir o eliminar algún riesgo identificado al inicio de la vigencia, el responsable del proceso deberá remitir una comunicación interna a la Oficina Asesora de Planeación, en el que se indique la justificación por la cual requiere que se realice la inclusión, modificación o eliminación del riesgo, quien realizara el análisis metodológico correspondiente.

- Se podrá llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos después de su publicación y durante el respectivo año de vigencia. En este caso, se debe realizar la solicitud por comunicación interna a la Oficina Asesora de Planeación con la sustentación pertinente y en congruencia con los aspectos generales relacionados sobre la identificación del riesgo.

- Siguiendo los lineamientos del DAFP en su Guía para la administración del riesgo y el diseño de controles en Entidades públicas, versión 5 (2020) para los riesgos de corrupción se precisan algunos lineamientos para la definición del impacto y las zonas de riego aplicables.

- Las responsabilidades de cada una de las líneas de defensa están detalladas en el numeral 3 de la presente guía, Responsables.

- El monitoreo y evaluación de controles por parte de la Oficina Asesora de Planeación, se realizará de acuerdo a la información contenida en el numeral 8.4.

- Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos antes de su publicación. Para lo cual la Oficina Asesora de planeación ejecutara actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos.

- Los riesgos clasificados en nivel de riesgo extremo y alto en zona de riesgo residual, deben tener un plan de acción definido, sobre el cual se asignan los responsables de su ejecución y se determinan los recursos, la periodicidad, la fecha de inicio y finalización, con el fin de asegurar su implementación.

  Para el caso de los riesgos de corrupción, de corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo, sin importar el nivel de riesgo residual en el que se ubiquen, deben contar con plan de acción.

- Los controles establecidos para cada riesgo, deben ser lo suficientemente eficaces para atacar la causa raíz, de esta manera efectuar una correcta mitigación del riesgo.

- En caso de encontrar que el tratamiento del riesgo requiere la participación de otro(s) proceso(s), el responsable del proceso deberá comunicar a los responsables de los procesos involucrados, con el fin de que se gestione el riesgo de forma concertada.

- Los activos de información deben ser analizados y establecidos por cada proceso.

- El diseño de acciones de prevención y mitigación de los riesgos deberá alinearse con los componentes de racionalización de trámites, de mecanismos para mejorar la atención al ciudadano, y de mecanismos para la transparencia y acceso a la información, especialmente con las acciones de racionalización que se establezcan para los trámites y OPAs que se consideren.

- El mapa de riesgos responde a la metodología descrita en la presente guía, lo que significa compromiso en su elaboración por parte de los líderes de proceso como responsables, así como de su implementación de acciones de mitigación y reporte de monitoreo oportuno y completo.

- La presente guía se basa en las orientaciones metodológicas establecidas en las guías o herramientas dispuestas para tal fin por el Departamento Administrativo de la Función Pública – DAFP y la Secretaría de Transparencia.

6. Intenciones Generales de la Alta Dirección para la Administración del Riesgo

El Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER adopta la presente guía como política de Administración del Riesgo, la cual establece los lineamientos para la gestión y mitigación de los riesgos definidos en la entidad, y a su vez la Alta Dirección declara las siguientes intenciones generales:

> *El Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, alineado con sus objetivos estratégicos y en cumplimiento de su misión y visión, se compromete a mitigar y administrar adecuadamente los riesgos estratégicos, de gestión, corrupción, seguridad de la información, fuga de capital intelectual, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo, de acuerdo con la metodología institucional adoptada para su gestión.*
>
> *La mitigación y administración adecuada de los riesgos será aplicable a todos los procesos de la Entidad, a los servidores públicos en el ejercicio de sus funciones, contratistas y proveedores, incluyendo los trámites, servicios y otros procedimientos administrativos – OPAs.*
>
> *Los niveles de aceptación del riesgo (capacidad, apetito y tolerancia), definición del nivel de probabilidad, calificación del impacto, tratamiento de los diferentes tipos de riesgos, su periodicidad de seguimiento, responsables y responsabilidades de las líneas de defensa, serán establecidas en la metodología institucional de administración del riesgo adoptada por el IDIGER.*
>
> *Con el fin de dar cumplimiento a los mencionado, la Alta Dirección asignará el talento humano y los recursos presupuestales y tecnológicos que garanticen la efectividad de la presente política.*

7. Identificación del riesgo

7.1 Conocimiento y análisis de la entidad

(Herramienta – Hoja 1- Punto de partida)

Para la identificación del riesgo, en primer lugar se debe partir del análisis y determinación de los factores, elementos y todas aquellas actividades críticas contenidas en el contexto interno y externo en el que opera la entidad, para ello se recomienda en primer lugar tomar en consideración la plataforma estratégica del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER:

Misión
El IDIGER emprende acciones y genera lineamientos para la gestión del riesgo de desastres y la adaptación al cambio climático, en el marco de la coordinación del SDGR-CC en el Distrito Capital, con el fin de proteger a las personas en situación de riesgo y lograr el desarrollo sostenible de Bogotá D.C.

Visión
En el 2030 el Distrito contará con mejores capacidades para gestionar el riesgo de desastres y los efectos del cambio climático, mediante la intervención del territorio y coordinación efectiva del SDGR-CC por parte del IDIGER, para la construcción de una ciudad resiliente.

También es importante analizar los objetivos estratégicos e identificar los posibles riesgos que afecten su cumplimiento y que puedan ocasionar su éxito o fracaso.

Objetivos estratégicos

- Coordinar a los actores del SDGRCC con lineamientos, mecanismos, instrumentos y espacios de participación, para fortalecer el conocimiento y la reducción del riesgo, el manejo de emergencias y desastres, así como las medidas de adaptación al cambio climático en el Distrito Capital.
- Fortalecer y promover el conocimiento del riesgo de desastres y efectos del cambio climático para la toma de decisiones frente a las medidas de reducción, manejo y adaptación en el Distrito de Capital.
- Modernizar el sistema de Información de Gestión de Riesgos y Cambio Climático con enfoque de escenarios
- Fortalecer la identificación y ejecución de acciones de reducción del riesgo al igual que las medidas de adaptación al cambio climático en Bogotá D.C.
- Fortalecer el manejo de emergencias, calamidades y/o desastres en el marco del SDGR – CC en Bogotá D.C.
- Implementar la estrategia del servicio a la ciudadanía y a los grupos de interés del IDIGER, brindando soluciones integrales para el acceso a la información y mejora en la prestación de los servicios, procurando calidad, calidez y oportunidad en armonía con los principios de transparencia, prevención y lucha contra la corrupción.
- Fortalecer los procesos estratégicos, de apoyo y evaluación mediante la implementación de lineamientos que soporten la gestión misional en cumplimiento de los objetivos institucionales en el marco de la mejora continua.

Los anteriores objetivos estratégicos de la entidad están definidos según la metodología SMART, lo que verifica su adecuada formulación, pues son específicos, medibles, alcanzables, relevantes y proyectados en el tiempo.

Esta primera etapa de identificación del riesgo también se fundamenta en la identificación de los factores internos y externos que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales:

Tabla No. 2 Factores internos y externos de riesgo

FACTORES INTERNOS Y EXTERNOS DE RIESGO	
CONTEXTO INTERNO	**CONTEXTO EXTERNO**
Modelo de operación por procesos: Falencias en la definición del modelo de operación por procesos; objetivo y alcance de los procesos inadecuado; inconvenientes en la operación de los procesos; pertinencia de los documentos asociados a los procesos y falta de claridad frente a la operación; relaciones entre procesos con inconsistencias; falta de conocimiento del modelo de operación por procesos (Documentos, políticas, prácticas de gestión). **Financieros:** Inadecuada programación y seguimiento	**Políticos:** Decisiones políticas que afecten la operación institucional; influencias políticas que pueden afectar la operación institucional; cambios de gobierno; decisiones administrativas nacionales y/o distritales. **Económicos y financieros:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.

presupuestal; inadecuados procesos de planeación y ejecución presupuestal; políticas internas de austeridad del gasto. **Personal:** Disponibilidad de personal con los conocimientos necesarios; capacidad del personal para dar respuesta a las funciones asignadas; retraso en los procesos a causa del desconocimiento de las funciones; debilidad de programas de bienestar laboral y capacitación; acciones u omisiones de los servidores que intervienen en la gestión; alta rotación de contratistas o poca continuidad de equipos de trabajo existentes. **Seguridad y salud en el trabajo:** Espacio físico, instalaciones, temperatura; conflictos en los equipos de trabajo; debilidad en las relaciones interpersonales; estabilidad laboral; remuneración laboral; política de ascenso; bajo nivel de participación de los servidores en procesos de formación y capacitación en SSST; planeación inadecuada del tiempo de trabajo; carga mental elevada; acoso laboral; pandemias. **Tecnología:** Integridad de datos; obsolescencia de los sistemas tecnológicos y modelos para la administración de la información con los que cuenta la entidad; sistemas tecnológicos que no se adaptan a la naturaleza institucional; poca agilidad y caídas en los sistemas; sistemas no integrados; inadecuado mantenimiento preventivo y correctivo de sistemas de información; retrasos en la modernización de sistemas de información; fugas de información. **Estratégicos:** Definición inadecuada del Direccionamiento Estratégico Institucional; planeación institucional que no corresponde con las necesidades del gobierno o con las condiciones de la entidad; falta de continuidad en planes y proyectos institucionales; operación inadecuada de los modelos de gestión; incumplimiento de lineamientos de gestión establecidos por el gobierno; vigencia de lineamientos de gestión establecidos; pertinencia de los lineamientos. **Comunicación interna:** Canales utilizados y su efectividad; integridad de la información; debilidades en la disposición y consulta de la información interna; calidad, vigencia y pertinencia de la información interna que se requiere para generar resultados; Debilidad en la implementación de las estrategias de comunicación informativa y organizacional; Debilidad o ausencia de canales de comunicación internos **Estructura organizacional:** Estructura orgánica; manual de funciones y responsabilidades; competencias y requisitos; multiplicidad de funciones concentradas en un sólo cargo o dependencia; cambios en la estructura y funcionamiento de las dependencias; asignación de nuevas funciones; ausencia de criterios para la definición de niveles de responsabilidad y autoridad; alta rotación en el nivel directivo; falencias de liderazgo por parte de los subdirectores y jefes de oficinas. **Ético:** Falta de ética de los servidores y/o contratistas en el desempeño de su labor; deficiencias en el proceso de selección al validar las competencias comportamentales **Seguimiento y medición institucional:** Inadecuados mecanismos de seguimiento y control; sobrestimación de los mecanismos de control dispuestos sin ser adecuados con las condiciones institucionales; interpretación errónea de normas que implican la implementación de mecanismos de control; observaciones erradas por parte de los actores de evaluación y seguimiento; falta de aplicación de los mecanismos de control establecidos.	**Sociales y culturales:** Políticas migratorias; desplazamiento; secuestros; extorsión; vandalismo y delincuencia común; corrupción social; terrorismo; declaratorias de emergencias con componente social; percepciones equivocadas de la operación institucional; coordinación interinstitucional; convenios interinstitucionales. **Tecnológicos:** Avances en tecnología, acceso a sistemas de información externos, gobierno en línea; evoluciones tecnológicas; modificación de plataformas tecnológicas; interrupciones en las redes de comunicación; vulnerabilidad en los sistemas de seguridad de la información; cambios tecnológicos que generen obsolescencia de los sistemas y modelos con que cuenta la entidad. **Ambientales:** Emisiones y residuos; energía, catástrofes naturales; desarrollo sostenible; situaciones de emergencias; cambios climáticos; contaminación; gestión de residuos; cambios normativos y de aplicabilidad institucional. **Legales y reglamentarios:** Normatividad externa (leyes, decretos, ordenanzas y acuerdos); nuevos criterios jurisprudenciales; cambios normativos nacionales o distritales. **Seguridad física:** Posibilidad de ocurrencia de eventos que afecten las instalaciones, bienes y procesos de la entidad. **Imagen:** Poca o nula credibilidad en la gestión institucional; percepción negativa de la gestión institucional por parte de las partes interesadas; publicidad negativa; acciones, decisiones y trámites errados; inadecuada atención al usuario.

Fuente: Adaptado de Función Pública, 2018

De igual forma, se recomienda tener en cuenta los siguientes resultados y mediciones que representan información importante para lograr los objetivos y resultados de la entidad:

- ✓ Resultados de las auditorías internas y externas
- ✓ Resultados de las actividades de rendición de cuentas
- ✓ Medición del desempeño institucional en periodos anteriores
- ✓ Medición de la satisfacción de grupos de valor en periodos anteriores

- **Seguridad de la información - Identificación de los activos**

(Herramienta – Hoja 4- Riesgo Seguridad Información)

En lo que concierne con los riesgos de seguridad de la información, adicional al análisis del contexto descrito en el numeral anterior, es importante tener en cuenta la conceptualización de los activos de información:

Tabla No. 3 Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización -Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Fuente: Adaptado de Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Nota: El formato TC-FT-138 Formato Inventario de Activos de Información, soporta de manera detallada la identificación dichos activos.

7.2 Puntos de riesgo

(Herramienta – Hoja 2 – Identificación del riesgo)

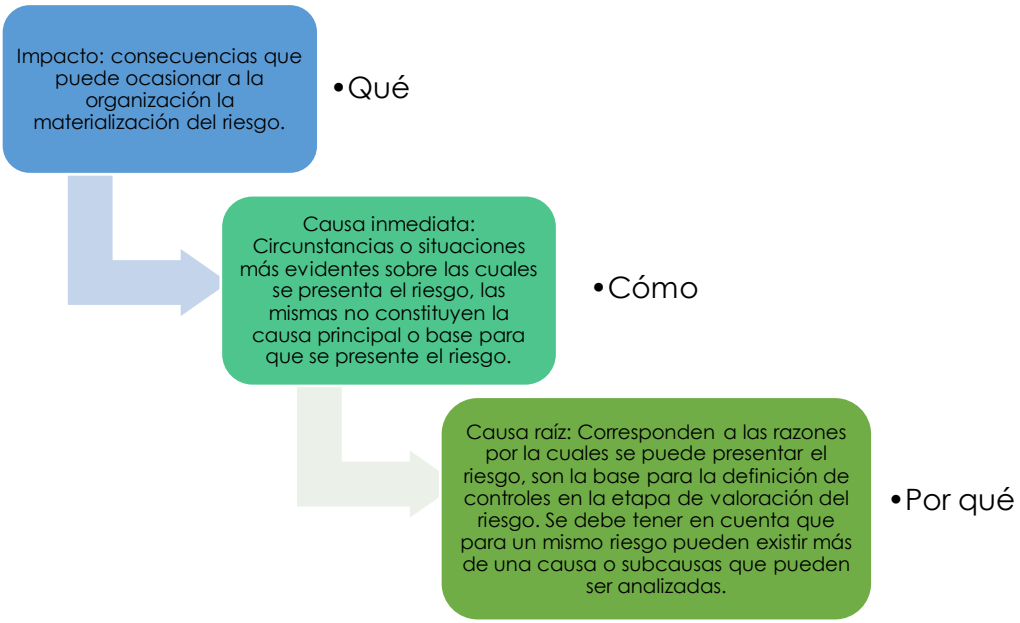
Complementario al análisis de la plataforma estratégica y del contexto interno y externo de la entidad, es importante que cada líder en compañía de su equipo de trabajo, pueda revisar al detalle cada una de las actividades que se ejecutan dentro del flujo de su proceso, y que presente evidencia o indicios de posible ocurrencia de riesgo.

7.3 Descripción del riesgo

(Herramienta – Hoja 2 – Identificación del riesgo)

Continúo al análisis del contexto de la entidad y la identificación de los puntos de riesgo, se procede a describir el riesgo, el DAFP en su guía para la administración del riesgo y el diseño de controles en Entidades Pública, V5 (2020), sugiere una estructura que permite el entendimiento del riesgo por parte de cualquier lector:

Figura No. 1 Estructura redacción del riesgo



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Se sugiere que todo riesgo descrito inicie con la frase "***Posibilidad de…***". A continuación se presenta un ejemplo claro de la correcta redacción de un riesgo identificado:

Impacto
Causa inmediata
Causa raíz

Posibilidad de afectación económica por multa y sanción del ente regulador debido a adquisición de bienes y servicios fuera de los requerimientos normativos

7.4 Área de impacto

(Herramienta – Hoja 2 – Identificación del riesgo)

En esta etapa, se hace fundamental identificar el área de impacto a la cual se ve expuesto el Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, en caso de la materialización de un riesgo:

- ✓ Económica (o presupuestal): afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimiento de tipo legal.

- ✓ Reputacional: afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio.

- ✓ Económica (o presupuestal) y reputacional: combina las afectaciones de ambos grupos de clasificación

- **Descripción riesgos de corrupción**

Para la correcta descripción de los riesgos de corrupción es necesario que además de la estructura mencionada en el numeral 7.3, contenga también cada uno de los siguientes componentes:

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

De igual manera, su descripción debe ser clara y precisa, no debe ser equivoca ni generar confusiones en el lector.

7.5 Tipo de riesgo

(Herramienta – Hoja 2 – Identificación del riesgo)

Es importante tener en cuenta la siguiente tabla durante la identificación del riesgo, la cual agrupa en categorías los diferentes riesgos que se puedan definir:

Tabla No. 4 Tipo de riesgo

Clasificación	Descripción
Estratégico	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos Entidad.
Gestión	Posibilidad de que una entidad incurra en pérdidas originadas por errores humanos, fallas tecnológicas o procesos, infraestructura, o por factores externos.
Corrupción	El riesgo de corrupción es la posibilidad de que por acción u omisión se use el poder para desviar la gestión de lo público en el beneficio privado.
Corrupción en los trámites y otros procedimientos administrativos – OPAs	La corrupción en trámites se puede presentar cuando se abren espacios de oportunidad, existen falacias en la integridad de quienes prestan el servicio y cuando hay presión de grupos externos.
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).
Fuga de capital intelectual	Posibilidad de pérdida de conocimiento organizacional existente por falta de mecanismos que permitan retener el conocimiento tácito y explícito tanto individual como grupal u organizacional.
Lavado de activos y financiación del terrorismo	Posibilidad de que una entidad incurra en pérdidas originadas por errores humanos, fallas tecnológicas o procesos, infraestructura, o por factores externos.

Fuente: Elaboración propia a partir de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

7.6 Clasificación del riesgo

(Herramienta – Hoja 2 – Identificación del riesgo)

La siguiente tabla muestra la descripción según la clasificación de los riesgos, además del posible factor de riesgo que pudo haberlo generado:

Tabla No. 5 Clasificación del riesgo

Clasificación	Descripción	Factor de riesgo
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	Proceso
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	Evento externo
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 están 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.	Talento humano
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.	Tecnología
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.	Pueden asociarse a varios factores
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.	Pueden asociarse a varios factores
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.	Infraestructura Evento externo

Fuente: Elaboración propia a partir de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

7.7 Capacidad, tolerancia y apetito del riesgo

(Herramienta – Hoja 2 – Identificación del riesgo)

Para comprender mejor este numeral, es conveniente repasar las siguientes definiciones:

- **Nivel de riesgo:** es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

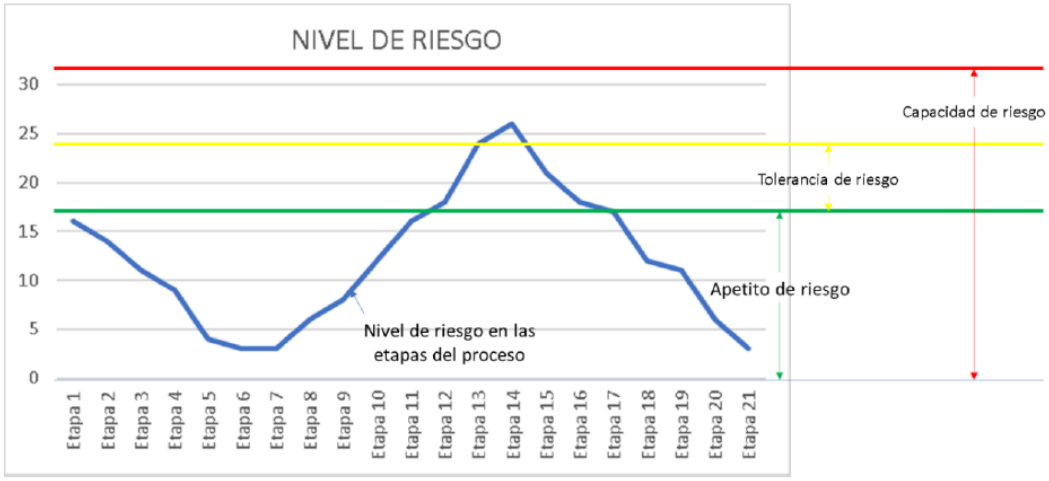
- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Tolerancia del riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección consideran que no sería posible el logro de los objetivos de la entidad.

La siguiente gráfica muestra la relación de las definiciones mencionadas:

Gráfico 1. Apetito, tolerancia y capacidad de riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Cada proceso debe determinar los valores de forma **cuantitativa** en intervalos para la capacidad, tolerancia y apetito de cada uno de los riesgos definidos, los cuales serán aprobados por la Alta Dirección en el Comité Institucional de Coordinación de Control Interno.

- Capacidad de riesgo: valor máximo valor del nivel del riesgo
- Tolerancia de riesgo: intervalo de valor igual o superior al apetito y menor o igual a la capacidad
- Apetito: intervalo de valor menor a la tolerancia de riesgo

Los valores definidos deben contener la justificación pertinente de la asignación de los mismos, según el análisis realizado por el proceso en relación con la aceptación del riesgo.

- **Seguridad de la información**

(Herramienta – Hoja 4 – Riesgo Seguridad Información)

Los riesgos identificados en seguridad de la información se clasifican dentro de las siguientes categorías:

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

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización (DAFP, 2020).

Nota: Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7 del anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas", el cual hace parte de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020 del DAFP.

8. Valoración del riesgo

Esta etapa de la gestión del riesgo, se desarrolla a partir de dos elementos fundamentales, que serán abordados en los siguientes numerales de la presente guía:

- Análisis de riesgos
- Evaluación de riesgos

8.1 Análisis de riesgo

En esta etapa de la gestión de riesgos, se establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de considerar el riesgo inherente (riesgo inicial).

8.1.1 Determinar la probabilidad

(Herramienta – Hoja 2 – Identificación del Riesgo)

La probabilidad de ocurrencia de los riesgos, se asocia a la exposición al riesgo del proceso o actividad sobre la cual se realiza el análisis, es decir, el número de veces que se pasa por el punto de riesgo en el periodo de un (1) año.

Lo anterior, significa que no existe subjetividad en este punto de análisis de probabilidad, pues determinar la frecuencia con la que se realiza cierta actividad debe ser claro.

La siguiente tabla muestra el porcentaje asignado de probabilidad según la frecuencia de ejecución de la actividad analizada:

Tabla No. 6 Criterios para definir el nivel de probabilidad en riesgos estratégicos, de gestión, fuga de capital intelectual y seguridad de la información

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

- **Determinar la probabilidad – Riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo**

(Herramienta – Hoja 2 – Identificación del Riesgo)

La probabilidad de ocurrencia en los riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo, puede ser analizada desde dos términos, la frecuencia o factibilidad, donde la primera corresponde al número de eventos en un periodo determinado, es decir, hechos que se han materializado o que cuentan con un historial de situaciones o eventos asociados al riesgo, y la segunda, analiza factores internos y externos que puedan generar el riesgo, es decir, un hecho que no se ha presentado, pero que es posible que suceda.

Tabla No. 7 Criterios para definir el nivel de probabilidad de riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo

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

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

8.1.2 Determinar el impacto

(Herramienta – Hoja 2 – Identificación del Riesgo)

Tal como se había mencionado en la etapa de identificación del riesgo de la presente guía, los impactos se definen dentro de dos grupos principales: impacto económico y/o reputacional.

La tabla No. 8 establece el % según el nivel de impacto a partir de los criterios para cada grupo principal.

Tabla No. 8 Criterios para definir el nivel de impacto riesgos estratégicos, de gestión, fuga de capital intelectual y seguridad de la información

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

- **Determinar el impacto - Riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo**

(Herramienta – Hoja 3 – Impacto Riesgo de Corrupción)

A través del siguiente cuestionario definido en la Guía de administración del riesgo y diseño de controles, V4 (2018) y que aún se mantiene vigente en la última versión de la guía, se puede determinar el área de impacto para este tipo de riesgos:

Tabla No. 9 Criterios para definir el nivel de impacto en riesgos de corrupción, corrupción en trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo

Si el riesgo de corrupción se materializa podría Sí/ No	
¿Afectar al grupo de funcionarios del proceso?	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?
¿Afectar el cumplimiento de metas y objetivos de la dependencia?	¿Dar lugar a procesos sancionatorios?
¿Afectar el cumplimiento de misión de la entidad?	¿Dar lugar a procesos disciplinarios?
¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?	¿Dar lugar a procesos fiscales?
¿Generar pérdida de confianza de la entidad, afectando su reputación?	¿Dar lugar a procesos penales?
¿Generar pérdida de recursos económicos?	¿Generar pérdida de credibilidad del sector?
¿Afectar la generación de los productos o la prestación de servicios?	¿Ocasionar lesiones físicas o pérdida de vidas humanas?
¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?	¿Afectar la imagen regional?

¿Generar pérdida de información de la entidad?	¿Afectar la imagen nacional?
¿Generar daño ambiental?	

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Nota: Si la respuesta a la pregunta ¿Ocasionar lesiones físicas o pérdida de vidas humanas? es afirmativa, el riesgo se considera catastrófico.

Una vez contestado el cuestionario anterior, se procede a definir el nivel de impacto según los criterios de la siguiente tabla:

Tabla No. 10 Criterios para definir el nivel de impacto en riesgos de corrupción, trámites, otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo

No. Preguntas afirmativas	Impacto	Descripción
1-5	Moderado	Genera medianas consecuencias sobre la entidad
6-11	Mayor	Genera altas consecuencias sobre la entidad
12-19	Catastrófico	Genera consecuencias desastrosas sobre la entidad

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Nota: El impacto para los riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs, siempre debe estar ubicado en las columnas "moderado", "mayor" y "catastrófico", dado que sus consecuencias siempre serán significativas; por lo cual para esta clase de riesgos no aplican los niveles de impacto leve y menor.

Y los relacionados con lavado de activos y financiación del terrorismo siempre debe estar ubicado en las columnas "mayor" y "catastrófico", según lo indica la Ruta metodológica para la implementación del SARLAFT en las entidades distritales.

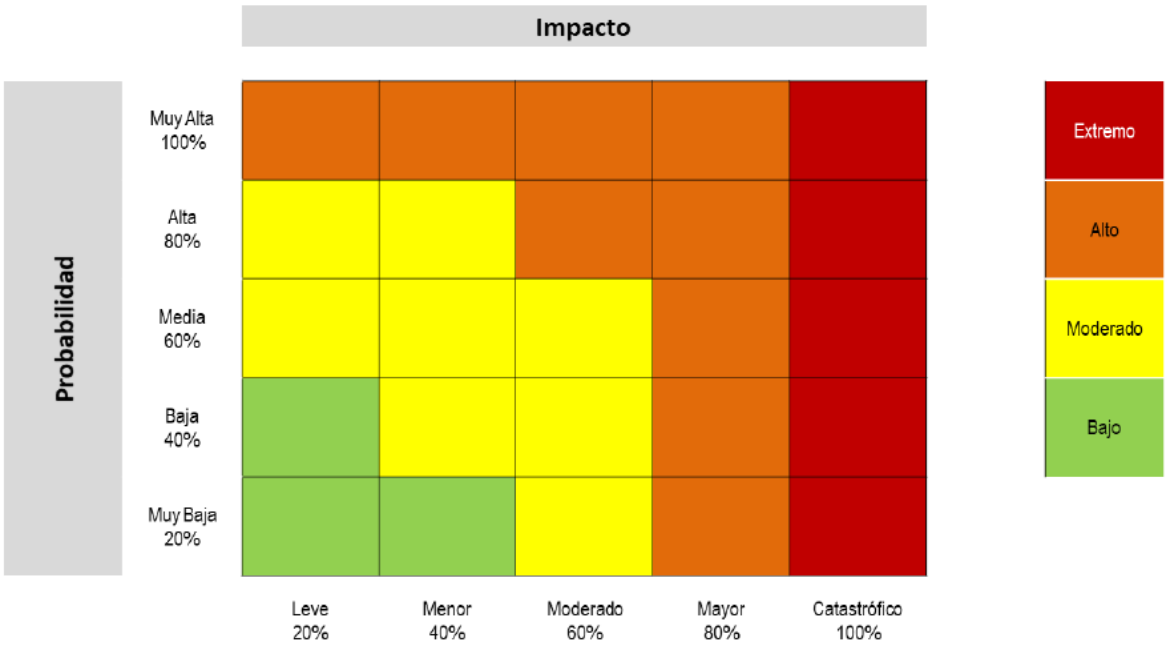
8.2 Evaluación de riesgos

8.2.1 Riesgo inherente

(Herramienta – Hoja 2 – Identificación del Riesgo)

En esta etapa de la gestión del riesgo, se determina la zona de riesgo inicial o nivel de riesgo de acuerdo a las combinaciones entre la probabilidad y el impacto determinadas en el paso anterior. Los niveles de severidad del riesgo están establecidos en la siguiente matriz:

Figura 2. Niveles de riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Nota: Los riesgos de de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo solamente pueden estar ubicados en las zonas de riesgo moderado, alto y extremo dentro del mapa de calor.

8.2.2 Valoración de controles

Con el fin de reducir o mitigar los riesgos definidos, los responsables de los procesos junto con su equipo de trabajo y bajo su criterio experto, identifican los controles a implementar y monitorear. Los siguientes numerales exponen la manera correcta para el diseño de los controles.

8.2.2.1 Estructura descripción de un control

(Herramienta – Hoja 5 – Valoración de Controles)

El Departamento Administrativo para la Función Pública establece en su guía para la administración del riesgo y el diseño de controles en entidades públicas, V5 (2020), la siguiente estructura para un correcto diseño del control:

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

A continuación se presenta un ejemplo claro de la correcta redacción del diseño de un control:

Figura No. 3 Redacción del control

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

8.2.2.2 Atributos para el diseño de controles de riesgos estratégicos, de gestión, fuga de capital intelectual y seguridad de la información

(Herramienta – Hoja 5 – Valoración de Controles)

Además de la estructura anterior, también es importante tener en cuenta cada uno de los siguientes atributos (de eficiencia o informativos) para el diseño adecuado de los controles de riesgos estratégicos, de gestión, fuga de capital intelectual y seguridad de la información:

Tabla No. 11 Atributos para el diseño de control de riesgos estratégicos, de gestión, fuga de capital intelectual y seguridad de la información

CARACTERÍSTICAS			DESCRIPCIÓN	PESO
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado. 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.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos. Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación. Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-

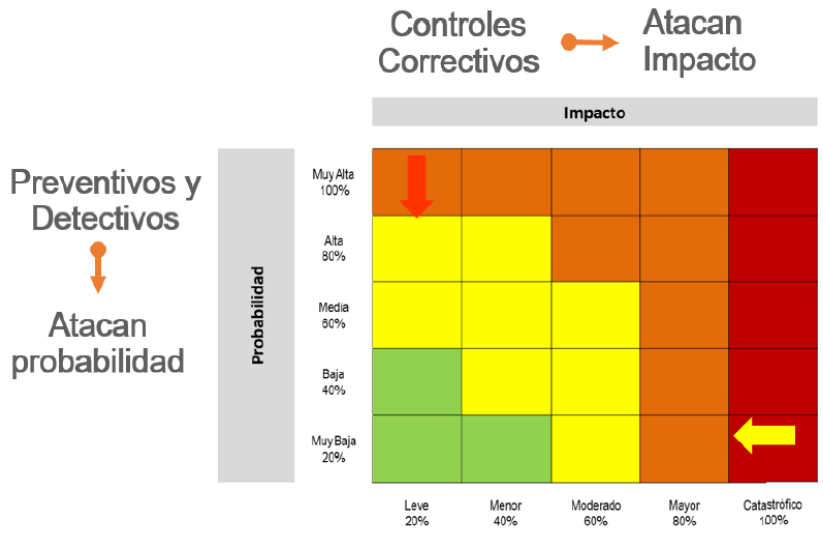
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos, estos no tienen una incidencia directa en su efectividad; sin embargo, es importante que todo control este documentado, se realice de forma continua, presente evidencia y ubicación de esta, tenga una fuente clara de información para la ejecución del mismo y se establezca de forma clara la manera de resolver las observaciones, desviaciones o diferencias identificadas durante la ejecución del control.

El siguiente mapa de calor presenta el desplazamiento entre filas y columnas según el tipo de control aplicado (preventivo, detectivo o correctivo):

Figura 4. Movimiento en el mapa de calor de acuerdo con el tipo de control



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Nota: Para los controles asociados a la seguridad de la información se debe emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.

8.2.2.3 Valoración de controles de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo

(Herramienta – Hoja 6 – Valoración Control Corrupción)

Al momento de calificar el control, se responderán las siguientes preguntas que establecen si el diseño del control es adecuado:

- Pregunta 1: ¿Existe un responsable asignado a la ejecución del control? ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?

El control debe iniciar con un cargo responsable o un sistema o aplicación, evitar colocar áreas de manera general o nombres de personas, el control debe estar asignado a un cargo específico.

- Pregunta 2. ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?

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

- Pregunta 3. ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, ¿etc.?

El control debe tener un propósito que indique para qué se realiza el control, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar), o detectar la materialización del riesgo, y conlleve a que se realicen los ajustes y correctivos en el diseño del control o en su ejecución.

- Pregunta 4: ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?

Cuando se esté evaluando el control, debemos preguntarnos, si la fuente de información utilizada ¿es información confiable?, el cómo se realiza la actividad de control.

- Pregunta 5: ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?

Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumple, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, debería gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones, el control tendría un problema en el diseño.

- Pregunta 6: ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?

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

8.2.2.3 Atributos de controles riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo

(Herramienta – Hoja 6 – Valoración Control Corrupción)

Los siguientes criterios permiten evaluar los controles de este tipo de, los cuales determinan si los controles existentes son fuertes, moderados o débiles:

Tabla No. 12 Criterios evaluación del diseño de controles riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo

CRITERIO DE EVALUACIÓN DEL DISEÑO	OPCIONES SEGÚN CRITERIO	PESO EN LA EVALUACIÓN DEL DISEÑO DE CONTROL
1.1 Asignación del responsable	Asignado	15
	No asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V4, 2018

- **Rango calificación del diseño de los controles en riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo**

Realizar el adecuado análisis y evaluación de los controles diseñados, permite detectar falencias en el diseño y ejecución, con el fin de mejorarlos en el caso de requerirse y obtener resultados realmente óptimos.

Tabla No. 13 Rangos calificación del diseño y la ejecución de los controles en riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo

Rango calificación del diseño	Resultado peso en la evaluación del diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V4, 2018

8.2.3 Riesgo residual

(Herramienta – Hoja 7 – Mapa de Riesgos General)

La efectividad de los controles aplicados al riesgo inherente, da como resultado la zona de riesgo residual. De esta manera, según el tipo de control aplicado (preventivo, detectivo o correctivo), se determina el desplazamiento dentro del mapa de calor en el eje de probabilidad y en el eje de impacto.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

El siguiente, es un ejemplo claro de la aplicación de controles de forma acumulativa propuesto en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020.

Tabla 14. Aplicación de controles para establecer impacto residual

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5, 2020

Nota: La herramienta de la entidad dispuesta para la gestión de riesgos está completamente formulada, sin embargo, la presente guía expone ejemplos claros para mejorar el entendimiento en cada etapa.

- **Riesgo residual en Riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo**

Cuando corresponda a un riesgo de corrupción, trámites, otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo, solamente hay disminución de probabilidad, no aplica el desplazamiento en el caso del impacto, es decir, para este tipo de riesgos no aplica el control correctivo.

Por ende, en los riesgos de corrupción la calificación del impacto de la zona de riesgo residual (después de controles), debe ser la misma de la zona de riesgos inherente (inicial o antes de controles) pues las consecuencias negativas en caso de presentarse algún evento de corrupción, no se pueden minimizar en comparación con los demás riesgos.

8.3 Tratamiento del riesgo

(Herramienta – Hoja 7 – Mapa de Riesgos General)

Con el fin de mitigar los riesgos, los responsables de cada proceso del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, deben tomar la decisión en materia de tratamiento del riesgo frente a un determinado nivel de riesgo residual, para lo cual se debe tener en cuenta la importancia del riesgo y el efecto que puede tener sobre la entidad, la probabilidad e impacto final y la relación costo – beneficio del tratamiento.

En las siguientes 3 categorías definidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, V5 (2020), se enmarca el tratamiento o respuesta dada al riesgo residual:

- ✓ Reducir: Después de realizar un análisis y considerar que el nivel de riesgo es alto o extremo, se determina tratarlo mediante transferencia o mitigación del mismo.

  Mitigar: Después de realizar un análisis y considerar los niveles de riesgo, se implementan acciones que mitiguen el nivel de riesgo, esta opción por lo general conlleva a un plan de acción.

  Transferir: Después de realizar un análisis se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

- ✓ Aceptar: Después de realizar un análisis y considerar que el nivel de riesgo es moderado o bajo, se determina asumir el mismo, con conocimiento de los efectos de su posible materialización.

- ✓ Evitar: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto o extremo, se determina NO asumir la actividad que genera este riesgo.

Nota: En el caso de riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo, estos no pueden ser aceptados.

8.3.1 Plan de acción

(Herramienta – Hoja 7 – Mapa de Riesgos General)

La presente guía estipula que los riesgos cuya valoración final (riesgo residual), se ubiquen en zona de riesgo extremo y alto, deben establecer un plan de acción que contenga como mínimo las siguientes condiciones:

- Acciones para mitigar el nivel de riesgo: descripción de las acciones a ejecutarse durante la vigencia, cada acción debe contener peso porcentual.
- Fecha de implementación: fecha de inicio y de finalización
- Formula del indicador: indicador que permita verificar el cumplimiento de cada acción
- Dependencia responsable: grupo o dependencia líder encargada de ejecutar el plan de acción

- **Riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo**

Todos los riesgos de corrupción, corrupción en los trámites y otros procedimientos administrativos – OPAs y los relacionados con lavado de activos y financiación del terrorismo, sin importar su nivel de riesgo residual, deben definir un plan de acción.

8.4 Monitoreo y seguimiento

(Herramienta – Hoja 8 – Seguimiento Cuatrimestral)

Se sugiere repasar la información del numeral Responsables (3) de la presente guía, donde está establecido los roles y responsabilidades de cada línea de defensa en lo que concierne con el monitoreo y seguimiento a los riesgos definidos en la entidad.

- **Monitoreo periódico**

Anualmente, como resultado del monitoreo, el líder de proceso deberá evaluar la pertinencia de los riesgos identificados y de las actividades de control formuladas, y definir las actualizaciones requeridas, de acuerdo a los cambios y el contexto interno y externo de la entidad.

Adicional, los líderes de proceso en conjunto con sus equipos de trabajo, deben monitorear y revisar mensualmente sus riesgos y si se da el caso ajustarlos. Lo anterior permite que el monitoreo del riesgo sea permanente y se verifique la efectividad de los controles propuestos

El monitoreo y la evaluación de los controles definidos para cada riesgo identificado, se efectuará cuatrimestralmente por parte de la Oficina Asesora de Planeación. El equipo de administración del riesgo de la Oficina Asesora de Planeación solicitará a los procesos el resultado del monitoreo realizado y generará un informe con observaciones y/o recomendaciones, buscando que se adopten las medidas de mejora o correctivas más adecuadas:

Tabla No. 15 Cronograma monitoreo y seguimiento

Número de reporte	Fecha de reporte por la primera línea de defensa	Fecha monitoreo OAP	Fecha seguimiento OCI
1er reporte	Dentro los (12) primeros días hábiles del mes de abril.	A partir del día hábil (13) y hasta el último día calendario del mes de abril.	Publicación informe en el link de Transparencia dentro de los primeros (10) días hábiles de mayo
2do reporte	Dentro los (12) primeros días hábiles del mes de agosto.	A partir del día hábil (13) y hasta el último día calendario del mes de agosto.	Publicación informe en el link de Transparencia dentro de los primeros (10) días hábiles de septiembre
3er reporte	Dentro los (12) primeros días hábiles del mes de diciembre.	A partir del día hábil (13) y hasta último día calendario del mes de diciembre.	Publicación informe en el link de Transparencia dentro de los primeros (10) días hábiles de enero

Fuente: Elaboración propia

Complementario a lo anterior, la Oficina Asesora de Planeación efectuara reuniones periódicas y extraordinarias, estas últimas en caso de requerirse, para el acompañamiento y asesoría metodológica a los líderes de los procesos y sus equipos de trabajo en la gestión de los riesgos definidos en el mapa de riesgos de la entidad.

- **Seguimiento**

La Oficina de Control Interno, como tercera línea de defensa deberá realizar seguimiento de manera independiente y objetiva a la gestión de riesgos definidos en el mapa de riesgos institucional, de acuerdo al Plan Anual de Auditorías y a la normatividad legal aplicable.

9. Materialización de los riesgos

En caso de materializarse un riesgo, los responsables de la Primera Línea de Defensa deben tener ya establecidas acciones de contingencia para implementar. Se debe informar a la segunda línea de defensa sobre la materialización detectada y revisar el detalle cada una de las etapas de la gestión del riesgo en el mapa de riesgos.

En caso que se requiera, se podrá solicitar apoyo metodológico a la Oficina Asesora de Planeación y se le comunicará la versión actualizada de su mapa de riesgos, para su consolidación en el mapa institucional.

Así mismo, a través de la segunda línea de defensa, se informara a la línea estratégica (Comité Institucional de Coordinación de Control Interno) para que desde allí se analice la situación y se den las orientaciones al respecto.

Cuando en el ejercicio independiente de auditoría, la Oficina de Control Interno identifique la materialización de un riesgo, deberá informar al líder del proceso sobre su detección y el líder deberá aplicar las acciones para la materialización del riesgo descritas anteriormente.

De igual manera la Oficina de Control Interno comunicará a la segunda línea de defensa sobre la materialización del riesgo y al Comité Institucional de Coordinación de Control Interno sobre el estado de los riesgos materializados en el ejercicio de las actividades de auditoría interna.

- **Materialización de riesgos de corrupción**

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

- ✓ Realizar la denuncia ante la instancia de control correspondiente, una vez surtido el conducto regular establecido dependiendo de su alcance.
- ✓ El líder de proceso verifica si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.
- ✓ La segunda línea de defensa informará a la tercera línea de defensa sobre la materialización del riesgo que hayan sido informadas por el líder del proceso.
- ✓ En articulación con la tercera línea de defensa, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.
- ✓ Realizar monitoreo permanente

10. Anexos

DE-FT-13 Mapa de riesgos institucional