Control de cambios

Versión	Fecha	Descripción de la modificación
01	01 diciembre 2010	Primera versión del Manual de Gestión del riesgo M-116302-02
02	1 marzo 2012	Cambio del tipo de documento, de código y modificación de las disposiciones: Actualización de glosario y normatividad, modificación de lineamientos, definición de competencias y responsabilidades, modificación de la metodología para la valoración de riesgos.
03	15 abril 2013	Inclusión de las instrucciones para la gestión de los riesgos de corrupción, inclusión de la calificación de los controles, actualización de marco normativo, modificación de zonas de riesgo, modificación de la definición de riesgo, incorporación de riesgo residual, eliminación de fuentes de riesgo, eliminación de evento predecible e impredecible, definición de control preventivo y correctivo.
04	14 marzo 2014	Se modifica la definición de causas de riesgo. Se incluyen disposiciones para los de 2014 riesgos ambientales y se aclaran las competencias del equipo SGI.
01	9 junio 2015	Modificación de la naturaleza del documento. Pasa de ser el Instructivo 1D-PGE- I013 al Manual de Gestión del Riesgo 1D-PGE-M4 Actualización del propósito Políticas de administración del riesgo: Se considera como tales la totalidad de los lineamientos establecidos en el presente manual, pues a lo largo de éste se da respuesta a lo establecido en la versión 2014 del Manual técnico del MECI al respecto. Cambio de la denominación de las etapas de gestión del riesgo Se establece cuál es la orientación de las acciones de tratamiento, la forma en la que se gestionarán los riesgos ambientales, los registros de las revisiones de las matrices de riesgos, los riesgos que deberán ser insumo para la revisión por la alta dirección, los cambios en la calificación de los riesgos con ocasión de su materialización, la definición de roles para la gestión de los riesgos de corrupción Clarificación de las competencias y responsabilidades Clarificación de la definición de corrupción y del Sistema de Gestión del Riesgo (glosario) Definición de la estructura de redacción de los diferentes elementos del riesgo Incorporación de directriz de modificación en la calificación del riesgo, como producto de su materialización Clarificación del seguimiento a los riesgos de corrupción Modificación de la denominación de las etapas de gestión del riesgo Modificación a la etapa de Evaluación de los riesgos y a los roles de la Oficina de Control interno Eliminación del Formato 1D-PGE-F038. Informe de seguimiento a la gestión de los riesgos
02	15 julio 2016	Incorporación de la política de gestión del riesgo vigente y clarificación de que se considera como políticas de administración del riesgo (operativas) la totalidad de los lineamientos establecidos en el presente manual, pues a lo largo de éste se da respuesta a lo establecido en la versión 2014 del Manual técnico del MECI al respecto. Precisión de competencias y responsabilidades Incorporación de los lineamientos generales para el subsistema de gestión del riesgo, en relación con: medición del desempeño del SGR,

Versión	Fecha	Descripción de la modificación
		Comunicación y consulta del SGR, Resolución de controversias y conflictos de interés, Incumplimiento del Subsistema de Gestión del Riesgo Cambio de la denominación de las etapas de gestión del riesgo Establecimiento de los contextos de riesgo de la SDG Precisión del contexto del riesgo y la manera en la que se articula con el contexto estratégico y cómo se evidencia en la gestión del riesgo Precisión de cada uno de los elementos de la gestión del riesgo de acuerdo con el área de impacto y establecimiento de la estructura de redacción de cada uno de ellos Clasificación de los riesgos de acuerdo con el área de impacto Inclusión de la valoración de la efectividad de los controles de los riesgos Inclusión de los controles detectives. Cambio de la valoración del riesgo en una estructura 3X3 a una estructura 5X5 (probabilidad e impacto) Incorporación del formato Reporte Monitoreo de riesgos 1D-PGE-F065 Incorporación de los planes de contingencia para los riesgos que tengan impacto las áreas consideradas críticas Incorporación del Mapa de riesgos Incorporación del perfil de riesgo Incorporación de herramientas y escenarios de articulación de todos los subsistemas del SGI, en torno a la gestión del riesgo – Figura de oficial de cumplimiento de subsistema de gestión, definición del rol de los subcomités técnicos y articulación de los oficiales de cumplimiento Inclusión de herramientas para la consolidación y análisis global de la gestión del riesgo. Reserva de derechos morales de autor: el presente documento ha tomado algunos elementos conceptuales del documento "Manual de gestión integral de riesgos" versión 3, de la ESE San Cristóbal, elaborado por los Ingenieros Patricia Ome, Alejandro Marín y Leonardo López Ávila.
01	**21 junio 2017**	Se crea la primera versión del documento bajo el modelo de operación por procesos vigentes, teniendo en cuenta que proviene del Manual de Gestión del Riesgo con código 1D-PGE-M004 en su versión 2. De manera general, se realizan los siguientes cambios en el documento: Se estructura la tabla de contenidos del manual, se complementan los términos y definiciones, se ajustan las convenciones s, Se transforma el concepto de contexto del riesgo a niveles de gestión del riesgo, se precisan funciones en los roles y responsabilidades, se incorpora la política de gestión del riesgo aprobada por la Alta Dirección, se ajusta el esquema del ciclo de la gestión del riesgo (la etapa de contingencia se aborda de manera distinta), se detalla el desarrollo de la etapa de contexto del riesgo, se precisan los resultados concretos obtenidos en cada etapa y su articulación con la herramienta de gestión del riesgo, cambio del esquema de la estructura general del riesgo, incorporación de los elementos complementarios dados por la guía para la gestión de riesgos de corrupción.
02	**29 diciembre 2017**	Se incluye la descripción del cálculo del perfil de riesgo con la incorporación de la explicación puntual de su fórmula matemática de una manera clara y sencilla dentro del Manual de Gestión de Riesgo en atención al plan de mejora 970 resultado de la auditoría de control interno realizada en el mes de julio de 2017.
03	**11 octubre 2018**	El documento es ajustado según lo establecidos en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, versión 3 en los roles y responsabilidades se realiza el ajuste de acuerdo con las líneas de defensa establecidas por el MIPG, se cambian las instancias frente a la administración del riesgo.

Versión	Fecha	Descripción de la modificación
04	24 mayo 2019	El documento es ajustado atendiendo las recomendaciones realizadas por la Oficina de Control Interno a través del documento "Informe comparativo para el Manual de gestión del riesgo de la Secretaria Distrital de Gobierno frente a los lineamientos emitidos por el Departamento Administrativo de la Función Pública" de diciembre 18 de 2018 y a lo establecido en la "Guía para la administración del riesgo y el diseño de controles en entidades pública, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 4 de octubre de 2018", se hace ajuste al documento en : el alcance, la terminología, en el capítulo de la estructura y valoración del riesgo, se incluyen funciones que ejerce la Oficina de Control Interno, el mapa de calor de la probabilidad e impacto del riesgo, actualización de la valoración del impacto ambiental, criterios para calificar el impacto riesgo de seguridad digital de la información, se organiza el documento de acuerdo con los pasos establecidos en la guía, se reclasifica la tipología y se actualiza el capítulo de comunicación y consulta.
05	30 noviembre 2020	El documento es ajustado en sus diferentes capítulos con el fin de brindar mayor claridad sobre cada uno de los lineamientos establecidos para la gestión del riesgo en la Secretaría Distrital de Gobierno. • Se incluyeron términos aplicables en el glosario. • Se organizó la estructura del documento siguiendo el orden de los pasos en la metodología para la gestión de riesgos y los diferentes elementos que se desagregan en cada uno de ellos. • Se incorporó tabla de relación sobre todos los elementos constitutivos de la política de gestión de riesgos. • Se verificaron las escalas de valoración tanto para probabilidad, impacto, riesgo inherente y riesgo residual. • Se realizaron ajustes en general de redacción para precisión de conceptos y lineamientos de la gestión del riesgo. • Se relaciona la interacción con otros procesos donde se deben manejar lineamientos establecidos a partir de manuales o procedimientos
06	22 diciembre 2021	De acuerdo con la guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 de la dirección de gestión institucional de fecha diciembre de 2020 expedido por el Departamento de la Función Pública se ajustas las definiciones de riesgos y otros conceptos, ajustes al presente manual: • En actualiza la etapa de identificación del riesgo, se estructura propuesta para la redacción del riesgo. • Se actualizan las tipologías de riesgo. • En ajusta la etapa de valoración del riesgo: se precisa análisis de probabilidad e impacto y sus tablas de referencia, así como el mapa de calor resultante. • Para el diseño y evaluación de los controles se ajusta tabla de calificación. • Se reubica y precisan las opciones de tratamiento del riesgo. • Se incluyen indicadores clave de riesgo. • Se precisan términos y uso relacionados con los planes de tratamiento del riesgo.
07	26 abril 2022	• Se incluye la metodología de evaluación de riesgos ambientales. Se realizan las siguientes modificaciones: Se ajusta el numeral 3 "Términos y definiciones"; se ajusta el numeral 8.3. "Paso 2: identificación del riesgo" numeral 8.3.5. "Clasificación del riesgo", se agregan lo riesgos ambientales; se ajusta el numeral 8.4.2 "Determinar el impacto" y se agregan los criterios para calificar el impacto ambiental, se agrega la tabla 12 "criterios para calificar el impacto en riesgos ambientales" y se agrega tabla 13 "nivel de daño en el impacto ambiental".

Versión	Fecha	Descripción de la modificación
		• Se modifica y ajusta la numeración de las tablas del documento.
08	**29 noviembre 2022**	• Se incluye la metodología de soborno. • Se ajusta la introducción, numeral 1 "Objetivo" y • Numeral 1.1 "Objetivos específicos". Se incluye un objetivo específico en relación con los riesgos de soborno. • Se ajusta el numeral 3 "Términos y definiciones". • Se incluye la Matriz de Riesgos de Soborno en la tabla 5: Política de Administración del Riesgo dentro del numeral 8.2 Política de Administración del Riesgo • Se incluye el numeral 10. Riesgos de soborno y se aclaran competencias y lineamientos frente a la gestión del riego. • Se modifica y ajusta la numeración del documento
09	**30 de octubre de 2023**	• Se relacionan los procedimientos PLE-PIN-P015 Administración y monitoreo de riesgos de gestión y corrupción; y PLE-PIN-P017 Gestión de los riesgos de seguridad de la información. • Se da orden, se simplifican y actualizan los capítulos y contenidos del manual. • Se incluyen conceptos sobre riesgos fiscales de acuerdo con la actualización de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas, del DAFP, Versión 6 de noviembre de 2022.

Método de Elaboración	Revisa	Aprueba
El documento es actualizado por el equipo de riesgos de la OAP, y revisado metodológicamente por la analista designada del Grupo de Planeación Institucional de la OAP.	**Jacobo Pardey Rozo** Profesional Riesgos OAP **Luisa Fernanda Ibagón Moreno** Profesional Riesgos OAP **Yamile Espinosa Galindo** Profesional OAP – Analista del proceso	**Gabriel Felipe Angarita Serrano** Líder Macroproceso Planeación Estratégica Caso HOLA No. **352697** Aprobado por el Comité Institucional de Coordinación de Control Interno

Tabla de contenido

Contenido

1. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DE RIESGOS DE GESTIÓN Y CORRUPCIÓN 13
2. INSTANCIAS FRENTE A LA ADMINISTRACIÓN DEL RIESGO 16
2.1. Comité Institucional de Gestión y Desempeño 16
2.2. Comité Institucional de Gestión y Desempeño 16
3. PASOS PARA LA ADMINISTRACIÓN DE RIESGOS 17
3.1. Conocimiento de la Entidad 18
3.2. Establecimiento de contexto 19
3.3. Paso 1. Política de Administración del Riesgo 21
3.3.1. Marco conceptual para apetito del riesgo 22
3.3.2. Determinación de la capacidad del riesgo 22
3.3.3. Determinación del apetito del riesgo 23
3.3.4. Tolerancia del riesgo 23
3.4. Paso 2: Identificación de riesgos de gestión y corrupción 23
3.4.1. Análisis de objetivos estratégicos y de los procesos 24
3.4.2. Identificación de los puntos de riesgo 24
3.4.3. Identificación de áreas de factores de riesgo 25
3.4.4. Descripción del riesgo de gestión 27
3.4.5. Premisas para la adecuada gestión del riesgo 28
3.4.6. Clasificación del riesgo 28
3.5. Paso 3: Valoración del riesgo. 30
3.5.1. Análisis de riesgos 30
3.5.2. Criterios de impacto 31
3.5.3. Criterios para calificar el impacto ambiental 33
3.5.4. Valoración de controles 34
3.5.5. Tipología de controles y los procesos 35
3.5.6. Análisis y evaluación de los controles - Atributos 36
3.5.7. Estrategias para combatir el riesgo 38
3.5.8. Herramientas para la gestión del riesgo 39
3.5.9. Monitoreo y revisión de riesgos de gestión y corrupción 39
4. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN 40
4.1. Riesgo de corrupción 40
4.2. Valoración de riesgos 42
4.3. Criterios para calificar la probabilidad 43
4.4. Análisis de impacto 43
4.5. Valoración de los controles – diseño de controles 45
4.6. Tratamiento del riesgo 45
4.7. Monitoreo de riesgos de corrupción 47
5. SEGUIMIENTO 48
6. RESPONSABILIDAD FRENTE A LA MATERIALIZACIÓN DE UN RIESGO 49
7. PERIODICIDAD DEL SEGUIMIENTO DE LA MATRIZ DE RIESGOS DE CORRUPCIÓN 49
8. ACTUALIZACIÓN DE LAS MATRICES DE RIESGOS DE GESTIÓN Y CORRUPCIÓN 49

9. SEGUIMIENTO OFICINA DE CONTROL INTERNO 50
10. MATERIALIZACIÓN DE RIESGOS DE CORRUPCIÓN 50
11. COMUNICACIÓN Y CONSULTA 51
12. LINEAMIENTOS SOBRE LA GESTIÓN DE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE SOBORNO 52
12.1. Gestión de riesgos de soborno 53
12.2. Generalidades acerca de los riesgos de soborno 55
12.3. Criterios para calificar la probabilidad 56
12.4. Análisis de impacto 57
12.5. Valoración y diseño de los controles. 59
12.6. Niveles de riesgo 61
12.7. Definición del mapa de calor de riesgos de soborno 62
12.8. Tratamiento del riesgo 64
12.9. Monitoreo de los riesgos de soborno 65
13. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 66
14. DOCUMENTOS RELACIONADOS 72
14.1. Documentos internos 72

Introducción

La gestión de riesgos se puede considerar como una herramienta fundamental, por su vínculo con todo el quehacer de las entidades del Sector Público; incluso, se podría afirmar que no hay actividad de la vida que no incluya la palabra riesgo. Por ello, la humanidad desde sus inicios ha buscado maneras de protegerse contra las situaciones que pueda acarrear la materialización de riesgos, desarrollando métodos para evitar, minimizar o asumir riesgos, mediante la definición de acciones específicas; a este ejercicio, se le denomina Administración de Riesgos.

El Estado Colombiano, mediante el Decreto 1537 de 2001 estableció que todas las entidades de la Administración Pública deben contar con una Política de Administración de Riesgos tendiente a dar un manejo adecuado del tema, con el fin de lograr, de la manera más eficiente, el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia que se pueda presentar.

Por consiguiente, la Secretaría Distrital de Gobierno toma como referente los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión (MIPG), Decreto 1499 de 2017, que integra los sistemas de gestión de calidad y de desarrollo administrativo; el cual crea un único sistema de gestión articulado con el sistema de control interno, y se actualiza y alinea con los mejores estándares internacionales, como son el modelo COSO 2013, COSO ERM 2017 y el modelo de las tres líneas de defensa, este permite la definición de funciones y deberes esenciales para la articulación y administración de los riesgos, de manera que a partir de esta herramienta se permita mejorar la efectividad de la gestión y el cumplimiento de los objetivos estratégicos.

El presente manual se basa en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" establecida por el Departamento Administrativo de la Función Pública, que orienta metodológicamente las etapas de identificación, análisis y valoración de los riesgos presentes en el desarrollo de las actividades propias de la SDG y establece las acciones que se deben ejecutar para mitigarlos.

De la misma manera, la Secretaría Distrital de Gobierno ha asumido la decisión estratégica de implementar un Sistema de Gestión Antisoborno -SGAS, que incluye la Matriz de Riesgos de Soborno, enmarcada en lo establecido por el Departamento Administrativo de la Función Pública -DAFP en lo relacionado metodológicamente con las etapas de identificación, análisis y valoración de los riesgos, en concordancia con los requisitos de la norma ISO 37001.

Objetivo

Establecer la metodología para realizar la gestión integral de los riesgos que afectan el logro de los objetivos estratégicos y de procesos de la Secretaría Distrital de Gobierno, a través de su identificación, análisis, valoración, definición de estrategias para gestionar integralmente los riesgos, su monitoreo y revisión periódica, en el marco del Modelo Integrado de Planeación y Gestión- MIPG

Objetivos específicos

- Establecer una adecuada administración del riesgo como base confiable para la toma de decisiones.
- Determinar las actividades que se deben realizar para administrar los riesgos, estableciendo para cada una los responsables.
- Desarrollar una adecuada identificación, análisis, valoración y manejo de los riesgos, independientemente de su naturaleza.
- Concientizar en todos los niveles de la entidad sobre la necesidad e importancia de identificar y tratar los diferentes tipos de riesgos.
- Proponer estrategias para la ejecución de planes de acción para mitigar los riesgos generados en el entorno digital.
- Implementar lineamientos operativos para realizar la gestión de los riesgos de corrupción asociados a los procesos y a las probables prácticas de soborno que impactan la gestión de la SDG.

Alcance

Los lineamientos definidos en este manual se aplican en todos los procesos en nivel central y Alcaldías Locales de la Secretaría Distrital de Gobierno, para una adecuada gestión de los riesgos de gestión por procesos, de corrupción, de soborno, de seguridad digital y de tipo ambiental.

Términos y definiciones

Los términos y definiciones que se encuentran en este documento están basados en la NTC ISO 31000-2018, GTC 137 (ISO Guía 73:2009) y la "Guía para la administración del riesgo y el diseño de controles en entidades públicas":

- **Acciones asociadas:** Son las que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), orientadas a fortalecer los controles identificados. Se deben formular acciones cuando se han identificado fallas en los controles después de realizar su calificación.

- **Administración de riesgos:** Conjunto de elementos de control que, al interrelacionarse, le permiten a la SDG evaluar aquellos eventos negativos, tanto internos como externos que puedan afectar o impedir el logro de los objetivos institucionales.

- **Activo digital:** En el contexto de seguridad digital de la información 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.

- **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.

- **Amenazas:** Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **Análisis del riesgo:** Establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente) y posterior a la definición de controles para prevenir la ocurrencia del riesgo (análisis del riesgo residual).

- **Asumir el riesgo:** Opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- Auditoría Interna de Gestión: Son todas las actividades y procesos sistemáticos, independientes y documentados para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de la auditoría.

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

- **Calificación del riesgo:** Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **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

- **Compartir o transferir el riesgo:** Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

- **Control:** Medida que permite reducir o mitigar un riesgo / acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

- **Control detectivo:** Acción o conjunto de acciones que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

- **Control preventivo:** Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

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

- **Corrupción:** Corresponde al uso del poder para desviar la gestión de lo público hacia el beneficio privado.

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos entidades o proceso no autorizados.

- **Evaluación del riesgo:** resultado del cruce cuantitativo de la calificación de impacto y probabilidad, para establecer la zona donde se ubicará el riesgo.

- **Evento:** Es un término que hace referencia a un hecho dado inesperadamente y modifica las circunstancias que rodean al mismo.

- **Evitar el riesgo:** opción de manejo donde se deben determinar acciones para continuar disminuyendo tanto probabilidad como el impacto, mediante el fortalecimiento de controles, optimización de procesos y el diseño de nuevos controles.

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

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

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

- **Definición de las fuentes de riesgos:** Es todo individuo, grupo humano, entidad, elemento físico, actividad o fenómeno del entorno de los cuales se pueden derivar situaciones o actos que podrían afectar las áreas de impacto de la SDG, la Secretaría definió las siguientes fuentes de riesgo.

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

- **Gestión del riesgo**: Actividad adelantada por la alta dirección de la SDG y demás personal para proporcionar a la administración un aseguramiento razonable para el logro de los objetivos.

- **Mapa de riesgo:** Representación de la ubicación de los riesgos en cada nivel de criticidad, a partir de la calificación de la zona de riesgo residual.

- **Mapa de riesgos de corrupción:** Herramienta metodológica para identificar un conjunto sistemático de situaciones de índole administrativa que, por sus características, pueden originar prácticas corruptas, orientan programas de prevención de la corrupción.

- **Materialización del riesgo:** ocurrencia del riesgo identificado.

- **Matriz de Riesgos:** Resultado de la aplicación de las fases de identificación, análisis, evaluación y tratamiento, en cada proceso en el formato establecido para tal fin.

- **Modelo Integrado de Planeación y Gestión - MIPG:** Es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos (Decreto 1499 de 2107).

- **Monitorear:** observar, analizar, verificar y evaluar los riesgos identificados, determinando el adecuado desarrollo de cada una de las etapas de administración y el nivel de cumplimiento y efectividad de los controles y acciones definidas.

- **Opciones de manejo:** Posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

- **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.

- **Parte interesada:** Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad. Parte interesada puede ser interna o externa de la organización.

- **Función de cumplimiento antisoborno:** Persona(s) con responsabilidad y autoridad para el funcionamiento del sistema de gestión antisoborno.

- **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 Gestión:** Posibilidad de que suceda algún evento calidad, credibilidad, buen nombre y reputación y seguridad digital de la información que puede tener impacto sobre el cumplimento de los objetivos, se expresa en términos de probabilidad y consecuencias.

- **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.

- **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.

- **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.

- **Riesgo ambiental:** Es la posibilidad de que en el desarrollo de la gestión institucional ocurra un evento que impacte negativamente el ambiente.

- **Soborno:** Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directa o indirectamente, e independientemente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.

- **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.

- **Valoración del riesgo:** Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir y si es necesario, las acciones a desarrollar para el fortalecimiento de controles.

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

Siglas

- **CIGD:** Comité Institucional de Gestión y Desempeño
- **DAFP:** Departamento Administrativo de la Función Pública
- **COSO:** Committee of Sponsoring Organizations of the Treadway Commission
- **COSO ERM:** Gestión Integral de Riesgos
- **MIPG:** Modelo Integrado de Planeación y Gestión
- **NTC:** Norma Técnica Colombiana
- **OAP:** Oficina Asesora de Planeación
- **PEI:** Plan Estratégico Institucional
- **SCI:** Sistema de Control Interno
- **SDG:** Secretaría Distrital de Gobierno
- **SDI:** Seguridad Digital de la Información

- **SIG:** Sistema Integrado de Gestión
- **SGAS:** Sistema de Gestión Antisoborno

1. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DE RIESGOS DE GESTIÓN Y CORRUPCIÓN

La administración del riesgo depende de la participación de la Alta Dirección y los colaboradores de la SDG. Es preciso identificar los diferentes roles y responsabilidades de los actores en la implementación, operación, monitoreo, seguimiento y fortalecimiento de la gestión del riesgo acorde con lo establecido en el Modelo Integrado de Planeación y Gestión - MIPG.

Frente a la administración de riesgos de gestión y corrupción se presentan los roles y responsabilidades de cada línea de defensa así:

Tabla 1. Roles y responsabilidades por líneas de defensa

LÍNEA	RESPONSABLES	ROLES Y ACTIVIDADES
LÍNEA ESTRATÉGICA Define el marco general para la gestión del riesgo yel control y supervisa su cumplimiento.	La alta dirección, el equipo directivo, a través del Comité Institucional de Gestión y Desempeño, el Comité Institucional de Coordinación de Control Interno, y el Oficial de Cumplimiento. (solo para Riesgo de Soborno)[1]	Le corresponde a la alta Dirección monitorear y revisar el cumplimiento a los objetivos de la SDG a través de las siguientes actividades: • Revisar los cambios en el "Direccionamiento Estratégico" y cómo estospueden generar nuevos riesgos o modificar los que ya se tienen identificados. • Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. • Hacer seguimiento en el Comité Institucional de Gestión y Desempeño y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones en auditoría interna. • Revisar el cumplimiento de los objetivos institucionales, de procesos e indicadores, identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando. • Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. • Aprobar la Política de Gestión del Riesgo y asegurarse de su permeabilización en todos los niveles de la SDG a través de

[1] Mediante la Resolución 0935 de 2022 se designó al cargo de Subsecretaria de Gestión institucional.

LÍNEA	RESPONSABLES	ROLES Y ACTIVIDADES
		una comunicación efectiva. Definir el marco general para la gestión del riesgo y supervisar el cumplimiento de la política de riesgos y los lineamientos de este manual.
1° LÍNEA DE DEFENSA Desarrolla e implementa procesos de controly gestión de riesgos através de suidentificación, análisis, valoración, monitoreo y tratamiento de riesgos.	A cargo de los líderes de los procesos, programas y proyectos de la entidad, Alcaldes y Alcaldesas Locales	Monitorear y revisar el cumplimiento de los objetivos institucionales y del proceso a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción a través de las siguientes actividades: • Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos. • Revisar permanentemente el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. • Revisar de forma permanente que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. • Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando. • Revisar y reportar la "Matriz de monitoreo de riesgos", los riesgos que se han materializado en su proceso, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. • Revisar los planes de mejora establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. • Revisar y hacer seguimiento al cumplimiento de las actividades y planes de mejora con relación a la gestión de riesgos. • Diseñar, implementar y monitorear los controles, además de monitorear los riesgos de manera permanente. • Promover el autocontrol y la autoevaluación por parte del equipo de trabajo a su cargo y generar las acciones de mejora continua que correspondan. • Desarrollar e implementar la metodología para la gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y tratamiento, reportando a la segunda línea los avances y dificultades.

LÍNEA	RESPONSABLES	ROLES Y ACTIVIDADES
2° LÍNEA DE DEFENSA Asegura que los controles y los procesos de gestión de riesgos implementados porla primera línea de defensa,estén diseñados apropiadamente y funcionen como se pretende.	Oficina Asesora de Planeación Supervisores e interventores de contratos o proyectos y comitésde contratación entre otros Les corresponde monitorear la gestión de riesgo y control ejecutada por la primera líneade defensa, la difusión y asesoría de la metodología, de tal forma que se asegure su implementación y aplicación. Para el caso de los riegos de soborno está a cargo de la Subsecretaría de Gestión Institucional.	Soporta y guía la línea estratégica y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción y de soborno a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos a través de las siguientes actividades: • Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar yapoyar en la actualización de las matrices de riesgos. • Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. • 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 determinar las recomendaciones y seguimiento para el fortalecimiento deestos. • Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas yactualizadas en los procedimientos. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos. Le corresponde a la Oficina Asesora de Planeación soportar y guiar a la línea estratégica y a la primera línea de defensa, en la gestión adecuada de los riesgos de procesos y de corrupción. Para los riesgos de soborno el Oficial de Cumplimiento contará con un profesional de apoyo para realizar el seguimiento como la segunda línea de defensa, así mismo para la difusión y asesoría de la metodología, de tal forma que se asegure su implementación y aplicación.
3° LÍNEA DE DEFENSA Proporciona información sobre la efectividad del S.C.I.,	Oficina de Control Interno Le corresponde realizar evaluación	Monitorea y revisa de manera independiente y objetiva validando que la línea estratégica, la primera y segunda línea de defensa cumplan con las responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como las tipologías de riesgos de la SDG, a través de las siguientes actividades:

LÍNEA	RESPONSABLES	ROLES Y ACTIVIDADES
a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.	independiente sobre la gestión del riesgo en la SDG, validando que las líneas estrategia, primera y segunda línea de defensa cumplan con su responsabilidad para ellogro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.	• Revisar los cambios en el "direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos y proponer modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción y los de soborno. • Revisar el adecuado diseño y ejecución 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. • Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la SDG o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. • Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas yactualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.

2. INSTANCIAS FRENTE A LA ADMINISTRACIÓN DEL RIESGO

Para asegurar una adecuada administración de riesgos de gestión y corrupción, se cuenta con instancias que permiten realizar seguimiento al cumplimiento de los lineamientos de la política de gestión de riesgos establecidos en este manual.

2.1. Comité Institucional de Gestión y Desempeño

Es el órgano rector y articulador de las acciones y estrategias que se desarrollen para la correcta implementación, operación, seguimiento y fortalecimiento del MIPG, como marco de referencia del Sistema de Gestión de la entidad, en términos de la gestión del riesgo, tiene la siguiente las responsabilidades:

- Aprobar y hacer seguimiento a las acciones y estrategias adoptadas para la gestión de riesgos.
- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de riesgos.

2.2. Comité Institucional de Gestión y Desempeño

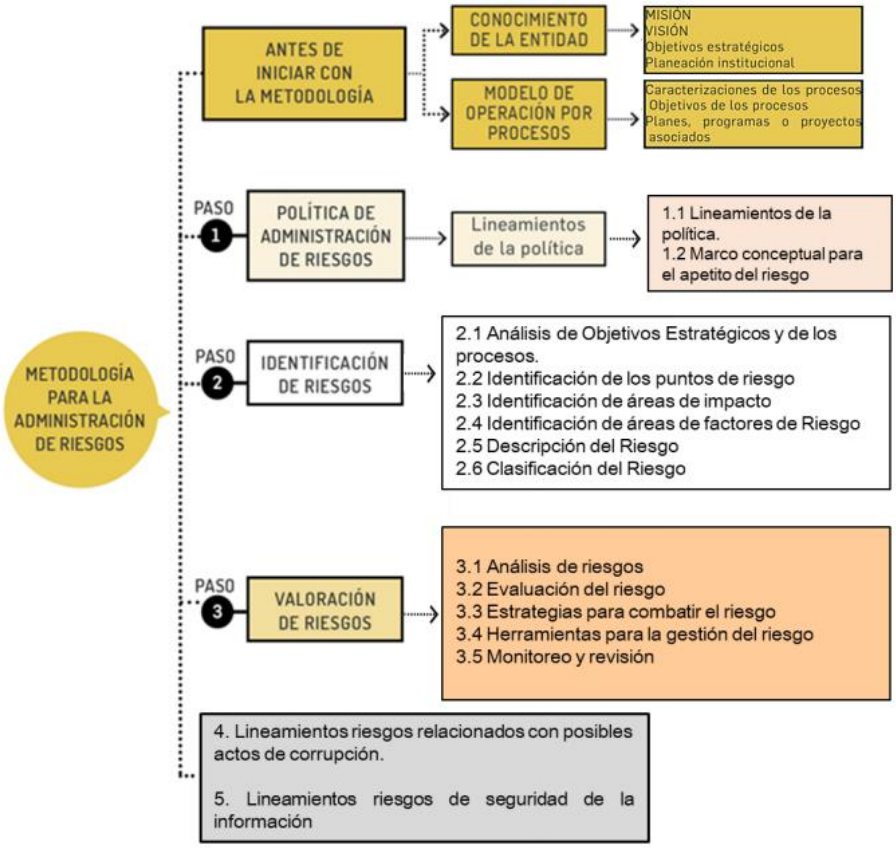
Es el órgano asesor e instancia decisoria en los asuntos de control interno que, en términos de la administración y la gestión del riesgo en la SDG, tiene la siguiente responsabilidad:

- Someter a aprobación de los miembros del comité la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

3. PASOS PARA LA ADMINISTRACIÓN DE RIESGOS

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Figura 1 Metodología para la administración del riesgo DAFP



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Función Pública, 2022.

Para el desarrollo de las diferentes etapas de la gestión de riesgos se deberán tener e0 cuenta los procedimientos PLE-PIN-P015 Administración y monitoreo de riesgos de gestión y corrupción y PLE-PIN-P017 Gestión de riesgos de seguridad de la información y dejar registro según corresponda en los formatos: PLE-PIN-F001 Formato matriz mapa de riesgos, PLE-PIN-F002 Formato matriz de riesgos de corrupción, PLE-PIN-F035 Formato matriz de monitoreo de riesgos, PLE-PIN-F042 Matriz mapa de riesgos seguridad de la información, PLE-PIN-F043 Matriz seguimiento a riesgos de corrupción y PLE-PIN-F054 Matriz de riesgos de soborno.

3.1. Conocimiento de la Entidad

La Entidad alinea su direccionamiento estratégico acorde a lo establecido en el Plan de Desarrollo Distrital y establece el Plan Estratégico Institucional donde se definen las prioridades estratégicas institucionales, tales como: misión, visión, objetivos estratégicos, valores, indicadores y metas; y se realizan de acuerdo con lo establecido en el procedimiento PLE-PIN-P009 Gestión del Plan Estratégico Institucional y la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC ISO31000).

La definición del contexto estratégico contribuye al control frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

En el "Procedimiento Gestión del Plan Estratégico Institucional PLE-PIN-P009" se establecen los lineamientos para la formulación del diagnóstico institucional y el análisis DOFA institucional, que sirve de insumo base para la formulación de análisis DOFA individual por proceso. A continuación, se relacionan los agentes generadores para tener en cuenta en el establecimiento del contexto:

3.2. Establecimiento de contexto

Tabla 2. Establecimiento del contexto

Establecimiento del Contexto Externo
Es el ambiente externo donde se determinan las características o aspectos esenciales del entorno en el cual opera la SDG, considerando los siguientes factores (entre otros): • **Políticos:** Cambios de gobierno, legislación, políticas públicas, regulación. • **Sociales Culturales:** Demografía, responsabilidad social, orden público. • **Legales y reglamentarios**. • **Tecnológicos:** avances en tecnología, acceso a sistemas de información externos, gobierno en línea. • **Financieros y Económicos:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. • **Ambientales:** Residuos sólidos, líquidos y gaseosos. • **Comunicación Externa:** mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la SDG.
Establecimiento del Contexto Interno
Es el entorno en el cual se determinan las características o aspectos esenciales del ambiente, en donde la SDG busca alcanzar sus objetivos considerando los siguientes factores: • **Estructura organizacional:** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo. • **Funciones y responsabilidades:** Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. • **Políticas, objetivos y estrategias implementadas.** • **Recursos y conocimientos con que se cuenta:** (económicos, personas, procesos, sistemas, tecnología, información). • **Relaciones con las partes involucradas.** • **Cultura organizacional:** Comunicación Interna. Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

- **Ambientales:** Residuos sólidos.
- **Financieros:** Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.

Establecimiento del Contexto del proceso

En este contexto se determinan las características o aspectos esenciales del proceso y sus interrelaciones considerando los siguientes factores:

- **Diseño del Proceso:** claridad en la descripción del alcance y objetivo del proceso.
- **Objetivo y alcance del proceso:** Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- **Transversalidad:** procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la SDG.
- **Interrelación con otros procesos:** Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- **Procedimientos asociados**: pertinencia en los procedimientos que desarrollan los procesos
- **Responsables del proceso:** Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- **Activos de seguridad digital del proceso**: Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.
- **Servicios tercerizados**: Todos aquellos servicios prestados por terceros que pueden afectar el objetivo del proceso.
- **Comunicación entre procesos**: Efectividad en los flujos de información determinados en la interacción del proceso.

El propósito de la matriz DOFA es establecer el contexto institucional del riesgo a partir de un análisis de las debilidades, oportunidades, fortalezas y amenazas teniendo en cuenta las condiciones internas y externas, las cuales se relacionan en el DOFA por proceso. A continuación, se presenta el esquema para la construcción de la matriz DOFA:

Tabla 3. Matriz DOFA

CONTEXTO INTERNO	
FORTALEZAS	**DEBILIDADES**
F_1	D_1
F_2	D_2
F_N	D_N
CONTEXTO EXTERNO	
OPORTUNIDADES	**AMENAZAS**
O_1	A_1
O_2	A_2
O_N	A_N

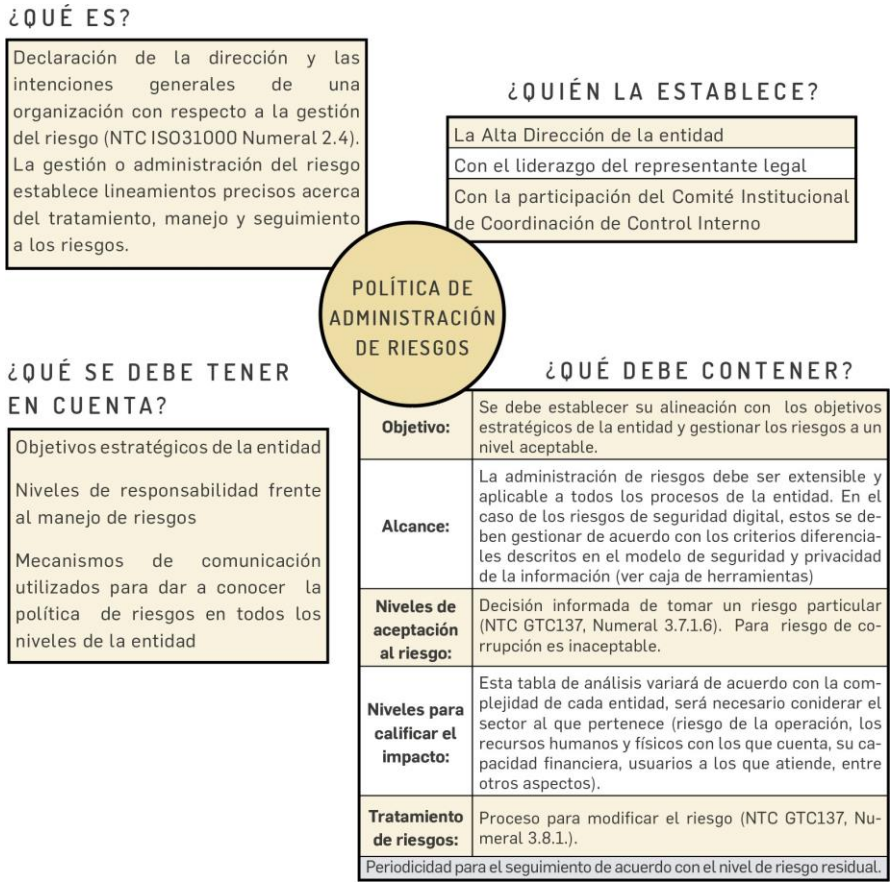
Fuente: Oficina Asesora de Planeación

Una vez se tiene el análisis DOFA por proceso (Hoja No. 1 PLE-PIN-F001 Formato matriz de riesgos) se debe partir de éste, para identificar el riesgo que pueda afectar de manera negativa el cumplimiento de los objetivos.

3.3. Paso 1. Política de Administración del Riesgo

La política de administración del riesgo hace referencia a las orientaciones, directrices documentadas y formalizadas que deben tenerse en cuenta para la gestión del riesgo en la SDG y que tienen como propósito evitar la materialización del riesgo.

Figura 2 Estructuración de la política de administración de riesgos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Función Pública, 2022.

La Alta Dirección de la Secretaría Distrital de Gobierno SDG manifiesta su compromiso y decisión de gestionar los riesgos a los que se encuentra expuesta, por medio de la **Política de Gestión del Riesgo** expresada a continuación:

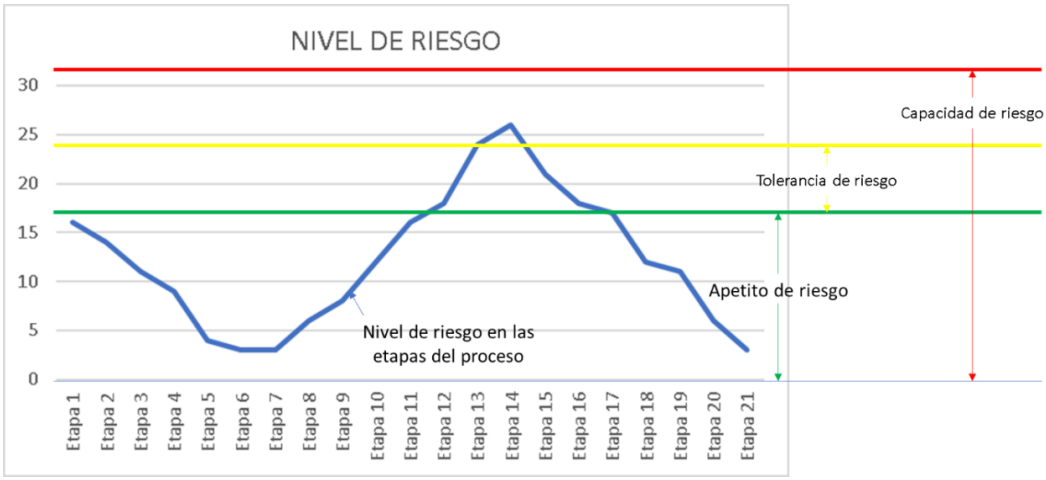
"La Secretaría de Gobierno se compromete a identificar, analizar, valorar y monitorear losriesgos que impidan el cumplimiento de los objetivos institucionales, con el apoyo de los servidores públicos, contratistas y la participación de la ciudadanía; alcanzando las metas trazadas de manera transparente y eficaz en la gestión de los procesos, la gestión ambiental, seguridad digital y la gestión de seguridad de la información, en pro del mejoramiento continuo de la Entidad".

3.3.1. Marco conceptual para apetito del riesgo

Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis:

Gráficamente los conceptos de nivel de riesgo, apetito de riesgo, tolerancia de riesgo y capacidad de riesgo se relacionan así:

Figura 3. Definiciones de apetito, tolerancia y capacidad de riesgo



Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

3.3.2. Determinación de la capacidad del riesgo

La entidad debe aplicar los valores de probabilidad e impacto contenidos en este manual y con base en esto debe determinar, con la participación y aprobación de la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno, definir los siguientes valores:

- Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
- Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina "capacidad de riesgo".

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

3.3.3. Determinación del apetito del riesgo

Luego de determinada la capacidad de riesgo por parte de la Alta Dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.

Este valor se denomina "apetito de riesgo", dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado 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.

3.3.4. Tolerancia del riesgo

La tolerancia de 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.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia.

3.4. Paso 2: Identificación de riesgos de gestión y corrupción

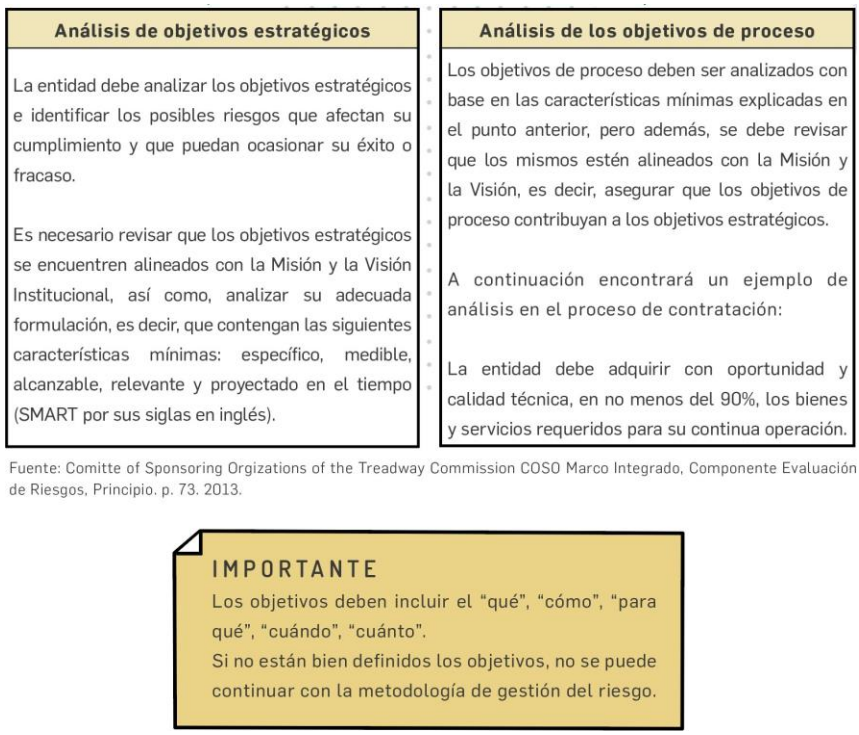
Esta etapa tiene como objetivo identificar los riesgos de gestión que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Se aplican las siguientes fases:

3.4.1. Análisis de objetivos estratégicos y de los procesos

Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

Figura 4 Análisis de objetivos



Fuente: Comitte of Sponsoring Orgizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio. p. 73. 2013.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Función Pública, 2022.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos.

3.4.2. Identificación de los puntos de riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Figura 5. Cadena de valor

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Función Pública, 2022.

Las áreas de impacto son la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

3.4.3. Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la Tabla 4 se encuentra un listado con ejemplo de factores de riesgo.

Tabla 4. Factores de riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los		Falta de procedimientos
			Errores de grabación, autorización

Factor	Definición		Descripción
	servidores de la organización.		Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurtos activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

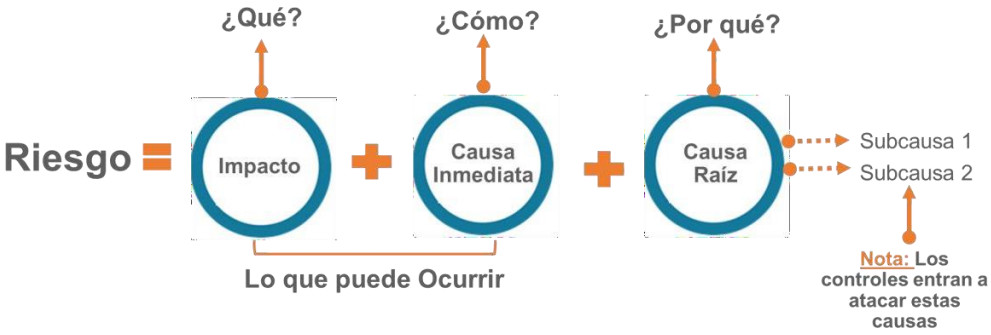
Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Función Pública, 2020.

3.4.4. Descripción del riesgo de gestión

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

Figura 6. Estructura propuesta para la redacción del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Función Pública, 2022.

- La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.
- Desglosando la estructura propuesta tenemos:
- Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

- Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de
- Controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

3.4.5. Premisas para la adecuada gestión del riesgo

- No describir como riesgos omisiones ni desviaciones del control.

  Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- No describir causas como riesgos.

  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- No describir riesgos como la negación de un control.

  Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.
- No existen riesgos transversales, lo que pueden existir son causas transversales.

  Ejemplo: pérdida de expedientes.

3.4.6. Clasificación del riesgo

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 5. Clasificación de riesgos

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
Ambientales	Alteración de un componente ambiental derivado de la implementación inadecuada de un control operacional.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

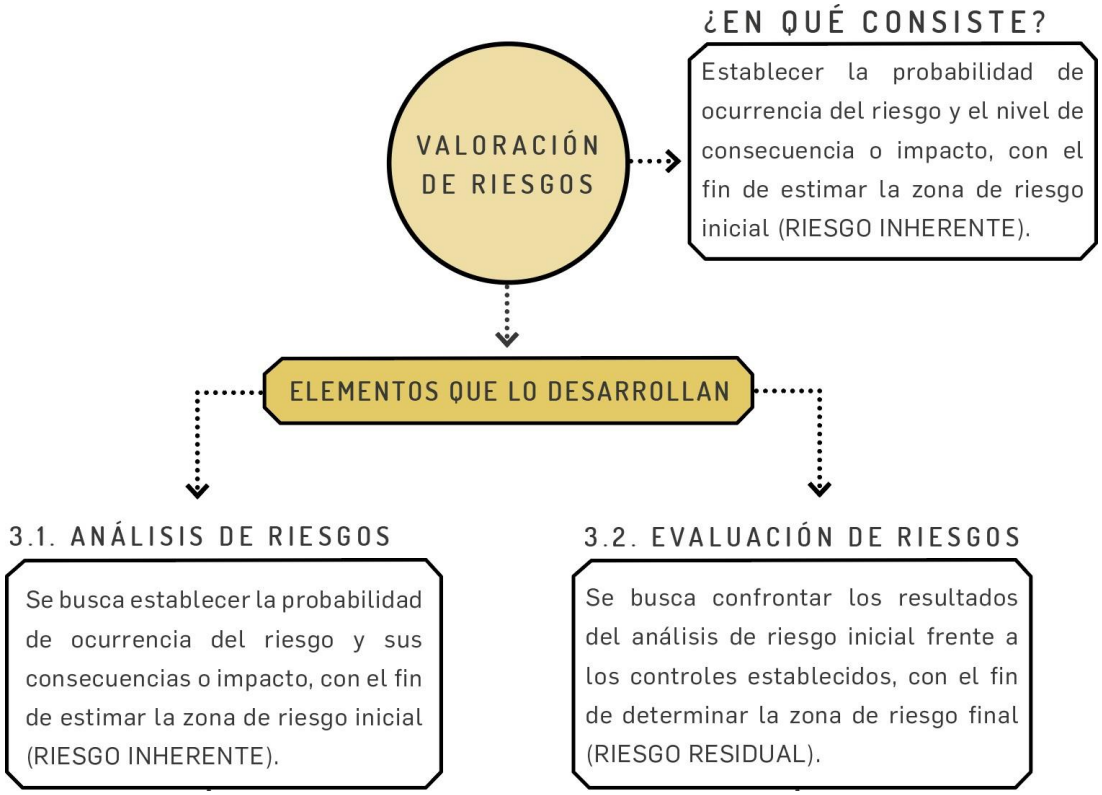
Teniendo en cuenta que en la tabla anterior se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

Figura 7 Relación ente factores de riesgo y clasificación del riesgo

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

3.5. Paso 3: Valoración del riesgo.

Figura 8. Estructura para el desarrollo de la valoración del riesgo



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

3.5.1. Análisis de riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos

tendrán la tendencia a quedar ubica dos en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Teniendo en cuenta lo anterior, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 6 se establecen los criterios para definir el nivel de probabilidad.

Tabla 6. Criterios para definir el nivel de probabilidad

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Función Pública, 2022

3.5.2. Criterios de impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la versión 2022 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP se contemplan afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional.

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

En la tabla 7 se establecen los criterios para definir el nivel de impacto.

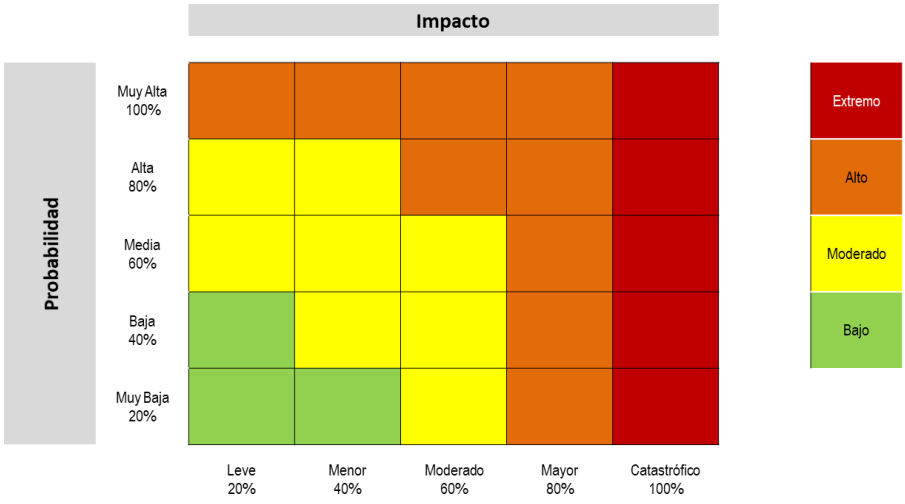
Tabla 7. Criterios para definir el nivel de impacto

	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, DAFP 2020.

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE), el cual trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor:

Figura 9. Matriz de calor (niveles de severidad del riesgo)



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

3.5.3. Criterios para calificar el impacto ambiental

El nivel de relevancia del impacto de los riesgos ambientales está dado por el producto del valor otorgado a los siguientes seis criterios de la escala de valor, siendo para cada uno 1, 5 o 10:

Tabla 8. Criterios para calificar el impacto en riesgos ambientales

No.	CRITERIOS DE VALORACIÓN	ESCALA DE VALOR		
1	Alcance Se refiere al área de influencia del impacto en relación con el entorno donde se genera.	Puntual 1 El impacto queda confinado dentro del área donde se genera.	Local 5 Trasciende los límites del área de influencia.	Regional o nacional 10 Tiene consecuencias a nivel regional o trasciende los límites del Distrito.
2	Probabilidad Se refiere a la posibilidad que se dé el impacto y está relacionada con la "REGULARIDAD" (Normal, anormal o de emergencia).	Baja 1 Existe una posibilidad muy remota de que suceda	Media 5 Existe una posibilidad media de que suceda.	Alta 10 Es muy posible que suceda en cualquier momento.
3	Duración Se refiere al tiempo que permanecerá el efecto positivo o negativo del impacto en el ambiente.	Breve 1 Alteración del recurso durante un lapso muy pequeño.	Temporal 5 Alteración del recurso durante un lapso moderado.	Permanente 10 Alteración del recurso permanente en el tiempo
4	Recuperabilidad Se refiere a la posibilidad de reconstrucción, total o parcial del recurso afectado por el impacto.	Reversible 1 Puede eliminarse el efecto por medio de actividades humanas tendientes a restablecer las condiciones originales del recurso.	Recuperable 5 Se puede disminuir el efecto a través de medidas de control hasta un estándar determinado.	Irrecuperable /irreversible 10 El/los recursos afectados no retornan a las condiciones originales a través de ningún medio.
5	Cantidad Se refiere a la magnitud del impacto, es decir, la severidad con la que ocurrirá la afectación y/o riesgo sobre el recurso.	Baja 1 Alteración mínima del recurso. Existe bajo potencial de riesgo sobre el recurso o el ambiente.	Moderada 5 Alteración moderada del recurso. Tiene un potencial de riesgo medio sobre el recurso o el ambiente.	Alta 10 Alteración Significativa del recurso. Tiene efectos importantes sobre el recurso o el ambiente.

No.	CRITERIOS DE VALORACIÓN	ESCALA DE VALOR		
6	Normatividad Hace referencia a la normatividad ambiental aplicable al aspecto y/o el impacto ambiental.	Baja 1 No tiene normatividad relacionada.	N/A	Alta 10 Tiene normatividad relacionada.

Fuente: Oficina Asesora de Planeación

De acuerdo con el resultado obtenido de la multiplicación de los seis criterios de valoración se determina el nivel de daño o afectación del ambiente de acuerdo con la siguiente escala:

Tabla 9. Nivel de daño en el impacto ambiental

AREA DE IMPACTO	IMPACTO	DESCRIPCIÓN
Ambiental	**Leve**	**Entre 1-12.500**
	Menor	**> 12.500 - 25.000**
	Moderado	**> 25.000 – 125.000**
	Mayor	**> 125.000 – 500.000**
	Catastrófico	**> 500.000 – 1.000.000**

Fuente: Instructivo Diligenciamiento de la Matriz de Identificación de aspectos y valoración de impactos ambientales, Secretaría Distrital de Ambiente – 2013.

3.5.4. Valoración de controles

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.

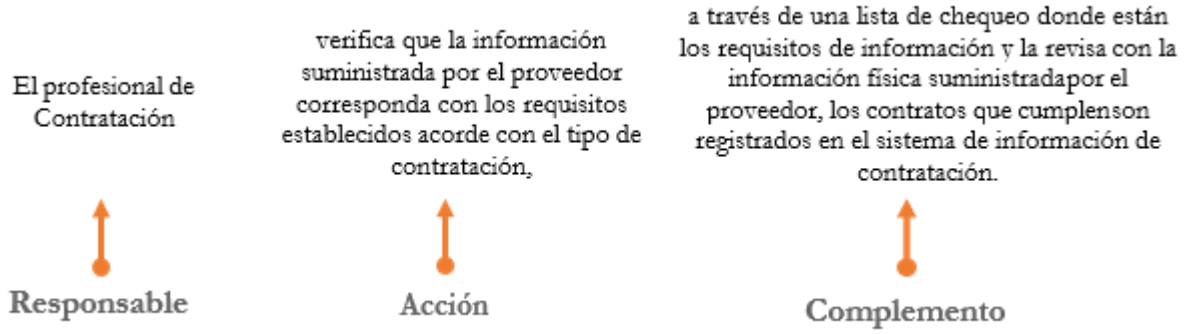
Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

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

- 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.
- Periodicidad: Frecuencia de ejecución de la acción de control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

En la figura 9 se establece un ejemplo bajo esta estructura.

Figura 9 Ejemplo aplicado bajo la estructura propuesta para la redacción del control

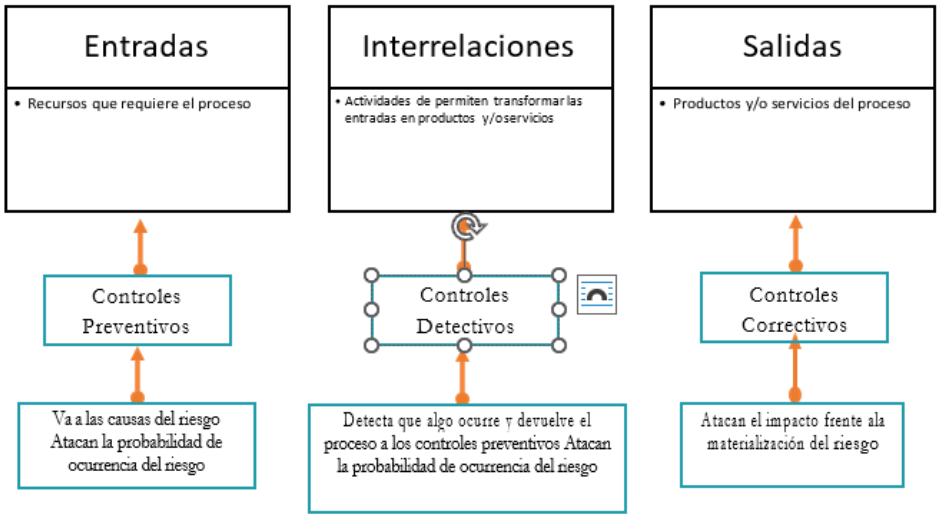


Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022.

3.5.5. Tipología de controles y los procesos

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura 10 se consideran 3 fases globales del ciclo de un proceso así:

Figura 10 Ciclo del proceso y las tipologías de controles



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

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

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

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

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

3.5.6. Análisis y evaluación de los controles - Atributos

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 10 se puede observar la descripción y peso asociados a cada uno así:

Tabla 10 Atributos de para el diseño del control

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%

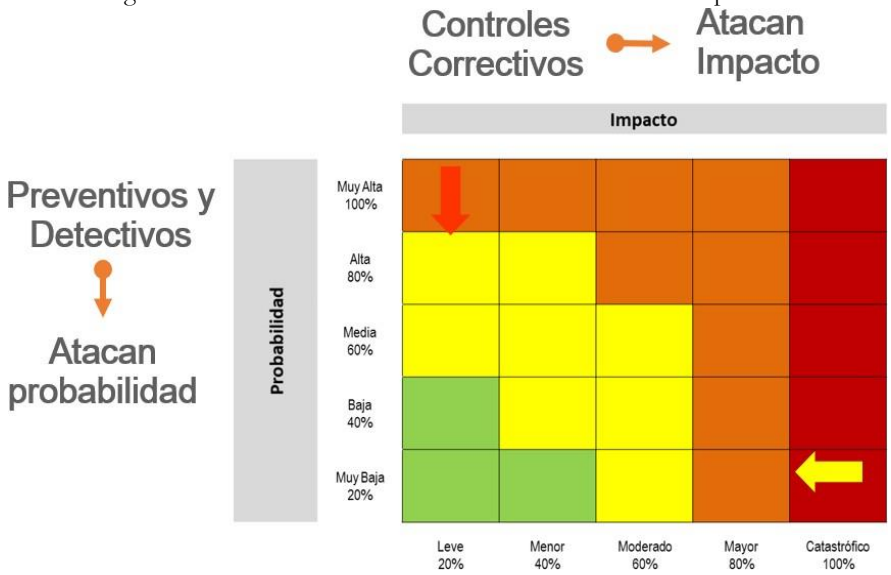
Características			Descripción	Peso
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan 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: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 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; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la figura 11 se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Figura 11 Movimiento en la matriz de calor acorde con el tipo de control



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

Para la aplicación de los controles se debe tener en cuenta que los 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.

Para la aplicación de los controles se debe tener en cuenta que los 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.

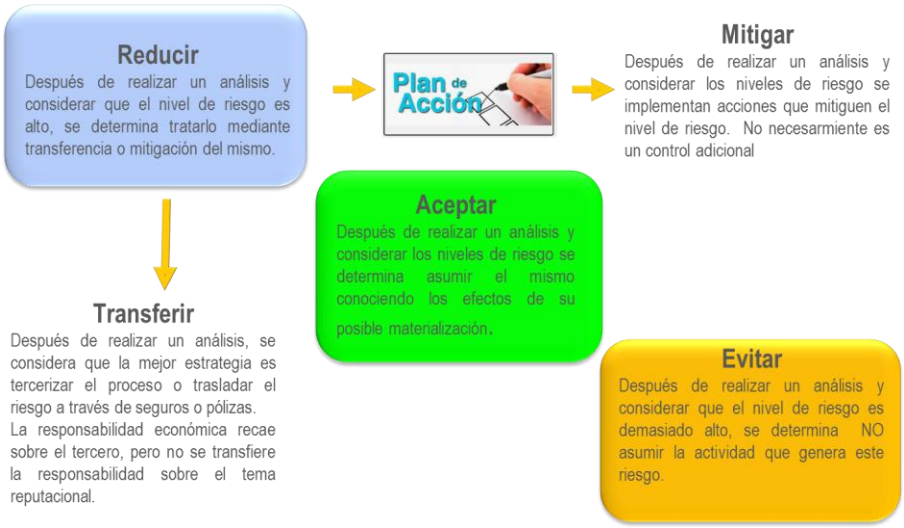
En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

3.5.7. Estrategias para combatir el riesgo

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

En siguiente figura 12 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Figura 12 Estrategias para combatir el riesgo



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

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

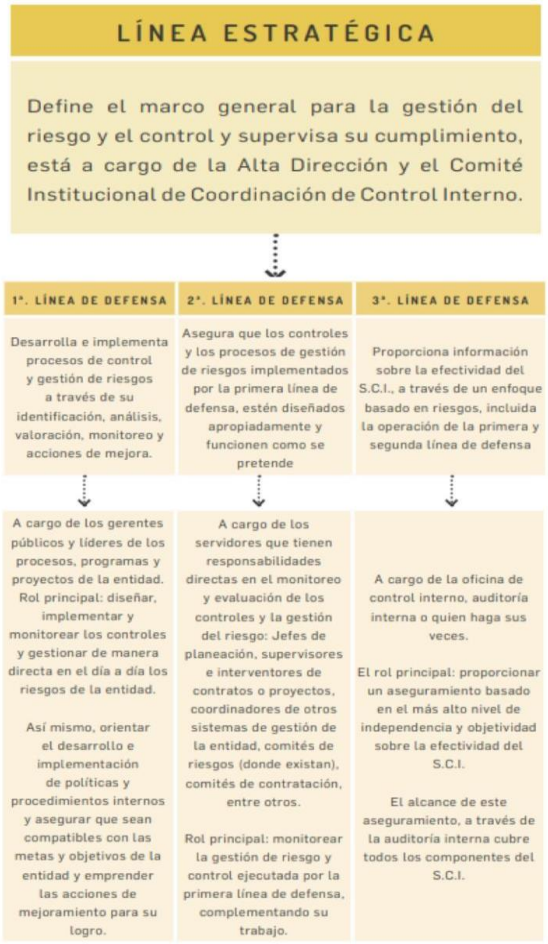
3.5.8. Herramientas para la gestión del riesgo

Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes: Gestión de eventos: un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

3.5.9. Monitoreo y revisión de riesgos de gestión y corrupción

El modelo integrado de planeación y gestión (MIPG) desarrolla en la dimensión 7 Control Interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en todos los servidores de la entidad como sigue:

Tabla 13 Esquema de líneas de defensa



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

La creación / actualización de matrices de riesgos de gestión y corrupción y el monitoreo realizado por la Oficina Asesora de Planeación se realiza de acuerdo con lo descrito en el PLE-PIN-P015 Administración y monitoreo de riesgos de gestión y corrupción.

4. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 5 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, del DAFP de 2020. Por lo anterior es necesario que, para formular el mapa de riesgos de corrupción, se remita a dicho documento.

4.1. Riesgo de corrupción

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

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

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

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

Los riesgos de corrupción se establecen sobre procesos.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

Tabla 11 Matriz definición de riesgo de corrupción

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

- Se elabora anualmente por cada responsable/ líder de los procesos junto con su equipo.
- La Oficina de Planeación le corresponde liderar el proceso de administración de estos riesgos. Adicionalmente, esta misma oficina es la encargada de consolidar el mapa de riesgos de corrupción.
- Se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.
- La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada.
- En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.
- En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

- Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la Oficina Asesora de planeación o diseñar y poner en marcha las 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 de corrupción.
- Así mismo, la Oficina Asesora de Planeación adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción.
- Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.
- Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.
- Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

4.2. Valoración de riesgos

Análisis de la probabilidad:

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

4.3. Criterios para calificar la probabilidad

Tabla 12. Criterios para calificar probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

4.4. Análisis de impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo Criterios para calificar el impacto en riesgos de corrupción:

Tabla 13. Preguntas para medir el impacto

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

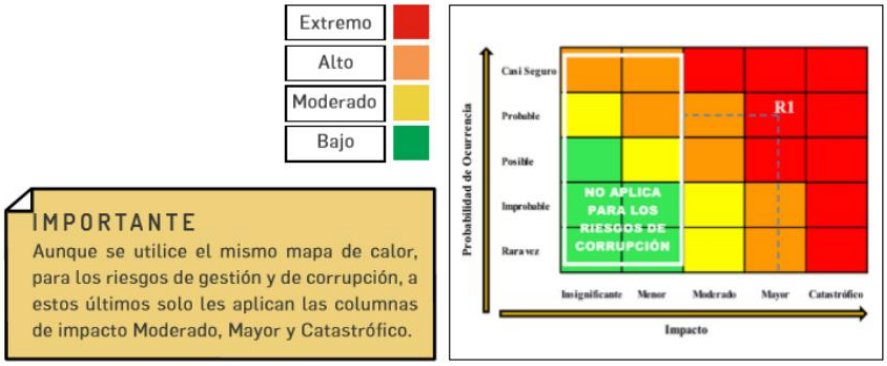
Nivel de impacto MAYOR

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

Figura 14. Mapa de calor



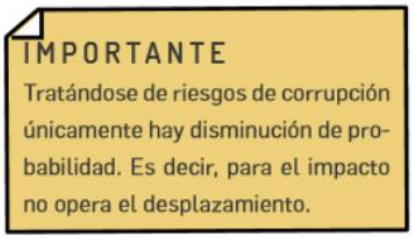
Fuente: Secretaría de Transparencia de la Presidencia de la República.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

4.5. Valoración de los controles – diseño de controles

Para el diseño y valoración de los controles, se deben tener en cuenta los parámetros señalados en la versión 5 de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" de 2020 del DAFP y en especial tener en cuenta lo establecido frente al Nivel del riesgo (riesgo residual):

Figura 15. Medición riesgos de corrupción



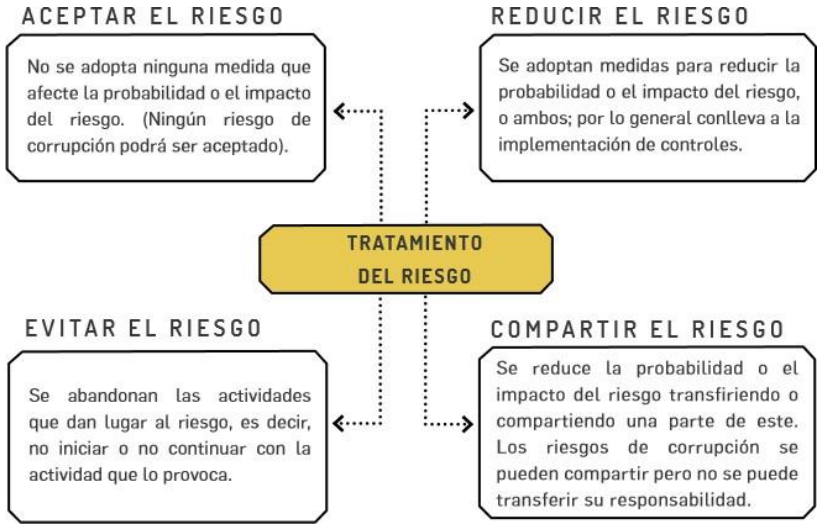
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

4.6. Tratamiento del riesgo

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo

derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

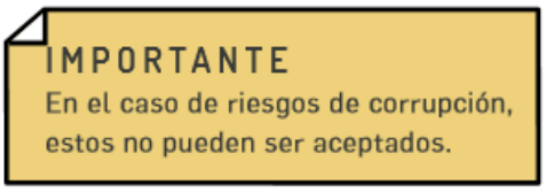
Figura 16. Tratamiento del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

- **ACEPTAR EL RIESGO**

Figura 17. No aceptación riesgos de corrupción



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

- **EVITAR EL RIESGO**

Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

- **COMPARTIR EL RIESGO**

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

- **REDUCIR EL RIESGO**

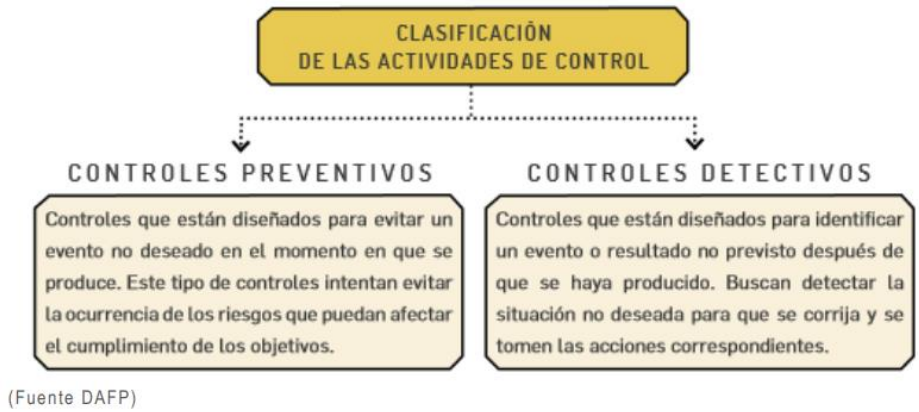
El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Tratamiento del riesgo – rol de la primera línea de defensa

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.

Figura 18. Clasificación controles



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP 2022

4.7. Monitoreo de riesgos de corrupción

Los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la Oficina de

Asesora de Planeación adelantar el monitoreo (segunda línea de defensa) para los riesgos de corrupción en la matriz que se establezca. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

Reporte de la gestión del riesgo de corrupción

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

5. SEGUIMIENTO

Corresponde a la recolección regular y sistemática de información para verificar, supervisar y observar de forma crítica o registrar el progreso de la gestión de riesgos en forma regular, a fin de identificar cambios sobre:

Tabla 14. Seguimiento a la metodología, monitoreo y periodicidad

MONITOREO		METODOLOGÍA DE SEGUIMIENTO	PERIODICIDAD
1	Ejecución de las acciones establecidas para realizar el tratamiento de los riesgos	A través de la revisión de los avances de los planes de tratamiento de acuerdo con las opciones de manejo para cada uno de los riesgos.	De acuerdo con la periodicidad establecida.
2	Comportamiento de los riesgos	A través de la revisión periódica de los riesgos potenciales y materializados de sus procesos y del monitoreo periódico que realizan Líderes de proceso y Alcaldes Locales.	Cuatrimestralmente
		Verificando la aplicación y efectividad de los controles dentro del proceso.	
		Para los riesgos de corrupción, la OAP consolida la información del comportamiento de los riesgos que reporten los líderes de cada proceso en las acciones de seguimiento al comportamiento y tratamiento de estos. Para los riesgos de soborno, la SGI consolida la información del comportamiento de los riesgos que reporten los líderes de cada proceso en las acciones de seguimiento al comportamiento y tratamiento de estos.	

Fuente: Oficina Asesora de Planeación

6. RESPONSABILIDAD FRENTE A LA MATERIALIZACIÓN DE UN RIESGO

Cada líder de proceso y/o Alcalde Local con el acompañamiento del promotor de mejora local y/o el referente ambiental (en el caso de las alcaldías locales), una vez se identifique la materialización del riesgo deberá inscribir el plan de mejoramiento correspondiente, siguiendo los lineamientos establecidos en el "GCN-M002 Manual para la gestión de planes de mejoramiento", dentro de los quince (15) días siguientes a la identificación formal de la materialización del riesgo (actas de mesas de trabajo, soporte de identificación propio de la ejecución del control, matriz de monitoreo de riesgos).

7. PERIODICIDAD DEL SEGUIMIENTO DE LA MATRIZ DE RIESGOS DE CORRUPCIÓN

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles, este seguimiento se deja registrado en el formato PLE-PIN-F043 Formato seguimiento matriz de riesgos de corrupción.

Los seguimientos se realizan de forma cuatrimestral así:

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

8. ACTUALIZACIÓN DE LAS MATRICES DE RIESGOS DE GESTIÓN Y CORRUPCIÓN

Los ajustes normativos o técnicos que deben orientar la actualización de las matrices de riesgos son los siguientes:

- Con la actualización del diagnóstico institucional la SDG deberá revisar la pertinencia de incluir los ajustes en las matrices de riesgo correspondientes.
- Cada vez que se materialice un riesgo identificado en la matriz de riesgos, se deberá actualizar para reflejar el comportamiento de los controles.
- La calificación de la probabilidad de ocurrencia del riesgo deberá ser revisada cuando se materialice el riesgo a fin de validar el incremento del nivel de probabilidad de acuerdo con los rangos definidos.
- Los riesgos que se encuentren incorporados en las matrices de la SDG se eliminarán en los siguientes casos:

- Que las causas que lo originen desaparezcan.
- El/los servicios al/a los que se asocia ya no sean responsabilidad de la SDG
- Alguno o todos los elementos del riesgo no corresponden con los criterios técnicos vigentes.

- En caso de que se realicen ajustes en los procesos y los objetivos establecidos en cada uno de ellos determinen cambios en la matriz de riesgos.
- El control de cambios de la matriz de riesgos debe contener la descripción clara de las inclusiones, eliminaciones o modificaciones realizadas a cada uno de los riesgos en cualquiera de los elementos de la identificación, análisis y valoración; de modo que permita realizar la trazabilidad de los cambios de la manera más precisa posible.
- Antes de la publicación, las matrices de riesgos deberán ser remitidas a la OAP – a través de un caso HOLA. Los analistas de la OAP realizarán la respectiva validación metodológica. Para el caso de los riesgos de soborno, esta validación previa está a cargo de la SGI.
- La revisión de las matrices de riesgos de corrupción deberá tener lugar al menos una vez al año.

9. SEGUIMIENTO OFICINA DE CONTROL INTERNO

La Oficina de Control Interno debe:

- Efectuar seguimiento a la gestión del riesgo, mediante la revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.
- Determinar la efectividad de los controles.
- Proponer acciones para mejorar la valoración de los riesgos.
- Proponer acciones para mejorar los controles establecidos para cada uno de los riesgos identificados.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo

Esta información sirve como insumo para analizar y validar la pertinencia de posibles ajustes tanto en los riesgos como en los controles que se encuentran identificados en cada uno de los procesos.

10. MATERIALIZACIÓN DE RIESGOS DE CORRUPCIÓN

El reporte de la existencia o materialización de los riesgos de corrupción por parte de los promotores de mejora de proceso se efectuará a través de la "Matriz monitoreo de riesgos" PLE-PIN-F035.

Las acciones que en caso de materialización de riegos de corrupción deben ser realizadas por el líder del proceso o alcaldes locales son:

- Informar a las autoridades competentes de la ocurrencia del hecho de corrupción para apertura de las investigaciones respectivas.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

11. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas, tanto internas como externas la Secretaría Distrital de Gobierno se hace durante las etapas apropiadas del proceso para la gestión del riesgo y a los lineamientos establecidos al interior de la entidad en el proceso de "Comunicación Estratégica".

Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación del servicio.

Tabla 15. Actividades a desarrollar para comunicar la Gestión de Riesgo

COMUNICACIÓN Y CONSULTA ASPECTO TRANSVERSAL	
1	Estrategias de comunicación en la SDG que se realizan a través de la intranet, correo institucional y actividades lúdicas.
2	Trabajo en equipo: la SDG dispone del cronograma de actividades reuniones a través de mesa de trabajo; este sistema permite garantizar que los riesgos estén correctamente identificados además la SDG reúne diferentes áreas de experticia para el análisis de los riesgos.
3	Conocimiento y análisis de la complejidad de cada uno de los procesos: la SDG a través de la intranet permite visualizar cada uno de los procesos con sus referencias, versiones y evidencias de su desarrollo.
4	Estrategias de comunicación externa para dar a conocer la gestión de riesgo a la ciudadanía, así como la recepción de opiniones sobre la gestión adelantada al interior de la entidad (comunicación de doble vía).

Fuente: Oficina Asesora de Planeación, SDG.

Las actividades de difusión y comunicación de manera permanente, utilizando los medios adecuados, garantizando la capacitación y/o entrenamiento de todos los colaboradores en cada uno de los pasos que componen la metodología de la administración del riesgo asegurando que permee a la totalidad de la Secretaría Distrital de Gobierno.

Tabla 16. Responsables para la información, comunicación y reporte

LÍNEA	RESPONSABLE	RESPONSABILIDAD PARA LA INFORMACIÓN, COMUNICACIÓN Y REPORTE
LÍNEA ESTRATEGICA	Comité Institucional de Coordinación de Control Interno	Establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.
1° PRIMERA LÍNEA DE DEFENSA	Jefe de área, líderes de procesos.	Asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.
2° SEGUNDA LÍNEA DE DEFENSA	El Jefe de Planeación Supervisores e Interventores de contratos y los líderes gestión de riesgos, Oficial de Cumplimiento, DTI	La difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la SDG, de tal forma que se asegure su implementación.
3° TERCERA LÍNEA DE DEFENSA	La Oficina de Control Interno	Realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la SDG, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la SDG el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

Fuente: Oficina Asesora de Planeación, SDG.

La comunicación de la información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

12. LINEAMIENTOS SOBRE LA GESTIÓN DE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE SOBORNO

La gestión de riesgos de soborno se desarrolla con base en los lineamientos de la Norma Internacional ISO 37001:2017- Sistema de Gestión Antisoborno, para tal efecto se establece la Matriz de Riesgos de Soborno PLE-PIN-F054 que responde a los requisitos de dicha norma. Para su comprensión a continuación, se hace una descripción de la metodología para su gestión.

Para la Gestión de Riesgo de soborno se establecen los siguientes roles y responsabilidades:

- Para la identificación de riesgos, análisis, evaluación del riesgo, identificación, diseño y evaluación de controles, cada proceso en cabeza del líder se encargará de organizar un equipo técnico de apoyo, bajo los lineamientos del Oficial de Cumplimiento del Sistema de Gestión Antisoborno basados en el presente manual.

- El/La Oficial de Cumplimiento del Sistema de Gestión Antisoborno designará un profesional, o un equipo de apoyo para revisar la matriz de riesgos una vez al año, junto con los equipos técnicos de cada proceso.

Para cumplir con el requisito de monitoreo cuatrimestral de los riesgos se definen las siguientes responsabilidades:

- La Primera Línea de Defensa en cabeza del líder de cada proceso quien puede delegar en su equipo para realizar el monitoreo dentro de los primeros 15 días de mayo, octubre y enero del año siguiente.

- La Segunda Línea de Defensa en cabeza Oficial de Cumplimiento del Sistema de Gestión Antisoborno realiza el Monitoreo a partir de día 16 de mayo, octubre y enero del año siguiente.

- La Tercera Línea de Defensa en cabeza del equipo de la Oficina de Control Interno podrá realizar auditorías internas a los riesgos de soborno cuando lo considere necesario.

12.1. Gestión de riesgos de soborno

Objetivo:

Determinar la metodología para la identificación, análisis, evaluación del riesgo, la identificación, diseño y evaluación de controles; mediante las cuales se determina el riesgo inherente, el riesgo residual y se determinan las acciones de tratamiento de los riesgos de soborno que permitan lograr los llevar a cumplir los objetivos estratégicos de la entidad.

Alcance:

La gestión de riesgos de soborno inicia con la identificación de los riegos hasta la implementación de controles de primera y segunda línea de defensa; además si es necesaria la implementación y seguimiento de Planes de tratamiento de riesgos residual medio y alto.

Para cumplir el alcance, los riesgos se asocian como el efecto de un evento sobre la incertidumbre relacionada con una actividad en la cual existe un posible hecho en el cual se puede materializar un evento de soborno, asumiendo la definición de soborno como la oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directa o indirectamente, e independientemente de su ubicación, en violación de la ley o requisitos aplicables, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las funciones u obligaciones de esa persona. En un hecho de soborno existe la incertidumbre en la cual dos o más personas en diferentes roles están expuestos ante el evento de soborno.

En la descripción del riesgo concurren componentes de su definición, así:

EFECTO DEL RIESGO + EXPOSICIÓN AL SOBORNO + ROL EXPUESTO AL SOBORNO + EL BENEFICIO PRIVADO+ INCUMPLIMIENTO

Los riesgos de soborno se establecen en los procesos, los cuales se identifican para cada procedimiento asociando los posibles eventos de incertidumbre frente a la exposición a cualquier practica de soborno.

El riesgo o los posibles eventos de incertidumbre de soborno deben estar descritos de manera clara y precisa, su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de soborno se ha diseñado una matriz de riesgos de soborno que aplica algunos aspectos metodológicos diseñados por el DAFP para los riesgos de corrupción.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de soborno:

Tabla 17. Matriz de definición de riesgo de soborno

Riesgo No.	Descripción	Ofrecer, prometer y entregar	Pedir o recibir
RS-1	Daño reputacional a la Secretaría Distrital de Gobierno por exposición a un evento de soborno de Directivos, Servidores, Contratistas, Constructores y Ciudadanía, en beneficio propio o de un tercero, por las prácticas de soborno sin cumplir los requisitos establecidos		**X**
2 RS-2	Riesgo de contagio por exposición a un evento de soborno de Directivos, Servidores, Contratistas, Constructores y Ciudadanía, en beneficio propio o de un tercero, sin cumplir los requisitos establecidos		**X**
3 RS-3	Deterioro a la imagen institucional por exposición a un evento de soborno de Directivos, Servidores, Contratistas, Constructores y Ciudadanía, en beneficio propio o de un tercero, sin cumplir los requisitos establecidos	**X**	
4 RS	Daño financiero al erario con la materialización de un evento de soborno con Directivos, Servidores, Contratistas, Constructores y Ciudadanía, en beneficio propio o de un tercero, sin cumplir los requisitos establecidos	**X**	
5 RS	Incumplimiento de la misión y los objetivos estratégicos de la SDG por la exposición a un evento de soborno, en beneficio propio o de un tercero, sin cumplir los requisitos establecidos		**X**

Fuente: Propia de la Secretaría Distrital de Gobierno

La Matriz de Riesgos de soborno presenta una hoja con las instrucciones y orientación en la Nota Técnica: para hacer más eficiente la gestión de riegos se indica: únicamente se deben digitar las tres columnas en color NARANJA, las columnas color VERDE son de selección tipo lista desplegable y las columnas color AZUL son automáticas, están ligadas a formulas, es decir en estas no se debe digitar ningún valor.

Para la identificación de los riegos de soborno se aplica los siguientes criterios:

Tabla 18. Matriz de Definición de Riesgo de Soborno

IDENTIFICACIÓN DEL RIESGO	**NÚMERO RIESGO**	RS 1
	PROCESO	COLUMNA TIPO LISTA: De todos los procesos de la SDG
	OBJETIVO DEL PROCESO	COLUMNA AUTOMÁTICA: Para cada proceso se asocian los objetivos aprobados en las caracterizaciones.
	DOCUMENTO DEL SISTEMA DE GESTIÓN SUSCEPTIBLE DE SOBORNO	COLUMNA PARA DIGITAR RESPUESTA: Código y nombre del documento del sistema de gestión susceptible a un hecho o evento de soborno

	ACTIVIDAD SUSCEPTIBLE DE SOBORNO	COLUMNA PARA DIGITAR RESPUESTA: Actividades susceptibles de soborno que realiza el equipo designado por el Líder de Proceso
	ROL INVOLUCRADO EN POSIBLE HECHO DE SOBORNO	COLUMNA TIPO LISTA: Los roles responden a los Grupos de Valor y Partes interesadas
	POSIBLE INCERTIDUMBE	COLUMNA AUTOMÁTICA: Se asocian las posibles acciones
	RIESGO	COLUMNA TIPO LISTA: que corresponden a los riesgos indicados en la tabla 19 Matriz de definición de riesgo de soborno.
	FUENTE DE RIESGO	COLUMNA TIPO LISTA: Personas, Tecnología, Procesos, Infraestructura, Externos (Eventos Naturales/ Terceros)
	ÁREA DE IMPACTO	COLUMNA TIPO LISTA: Calidad, Ambiente, Información, Servidor público o contratista o Credibilidad, buen nombre y reputación.
	CAUSAS DEL RIESGO	COLUMNA TIPO LISTA: Faltan puntos de control en el procedimiento, La Subcultura de la corrupción y el fraude, Falta de controles antisoborno de primera línea de defensa , La subcultura de hacer trámites y gestiones de manera fraudulenta, Debilidades del proceso de selección de Directivos y Servidores frente a la norma ISO 37001:2017 o Indebida injerencia política en asuntos internos
	CLASIFICACIÓN DE LA CAUSA	COLUMNA TIPO LISTA: Interna o Externa
	NIVEL ORGANIZACIONAL	COLUMNA TIPO LISTA: Estratégico, táctico, operativo
	CONSECUENCIAS FRENTE AL SISTEMA DE GESTIÓN ANTISOBORNO	COLUMNA TIPO LISTA: Deterioro de la función social del Estado y de la SDG. Así: Enriquecimiento ilícito y riesgo de contagio en la institución, Posible riesgo de contagio por prácticas indebidas en la institución, Enriquecimiento ilícito y riesgo de contagio en la institución, Posible materialización de conductas indebidas y de prácticas de soborno Posible materialización de prácticas de soborno, corrupción y fraude

Fuente: Subsecretaría de Gestión Institucional, SDG.

12.2. Generalidades acerca de los riesgos de soborno

- La Matriz de Riesgo de Soborno PLE-PIN-F054 se elabora una primera vez y se actualiza una vez al año por cada responsable/ líder de los procesos junto con su equipo de trabajo.
- Consolidación: A la Subsecretaría de Gestión Institucional le corresponde liderar el proceso de administración de estos riesgos. Adicionalmente, esta misma área será la encargada de consolidar el mapa de riesgos de soborno.
- Publicación del mapa de riesgos de soborno: Se publicará en la página web de la entidad, en la sección establecida para tal fin. La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. Dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los

artículos 18 y 19 de la Ley 1712 de 2014; en este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

- Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de soborno antes de su publicación. Con este propósito, la Subsecretaría de Gestión Institucional pondrá en marcha las 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 de soborno.
- Así mismo, se adelantará las acciones para que la ciudadanía y los grupos de valor externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de soborno.
- Se dejará la evidencia del proceso de socialización y publicación.
- Ajustes y modificaciones: Se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar la Matriz de Riesgos de Soborno después de su publicación y durante el respectivo año de vigencia. En este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas. Los ajustes que se generan se presentan al Comité Institucional de Coordinación de Control Interno antes de publicar una nueva versión en los primeros 3 meses de cada año.
- Monitoreo primero línea de defensa: En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo cuatrimestral a la gestión de riesgos de soborno, bajo los lineamientos de (la) Oficial de cumplimiento y su apoyo técnico.
- Monitoreo Segunda Línea de Defensa: El Oficial de Cumplimiento designará a un equipo de la Subsecretaría de Gestión Institucional para realizar el monitoreo a la Matriz de Riesgos de Soborno. Los resultados serán reportados a la Alta Dirección y se escalan al Comité Institucional de Coordinación de Control Interno según corresponda.

12.3. Criterios para calificar la probabilidad

La probabilidad de ocurrencia de los riesgos de soborno se califica con base en frecuencia de ocurrencia de un evento de soborno.

Tabla 19: Criterios de calificación de probabilidad de Riesgos de Soborno.

NIVEL	PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
1	RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
2	IMPROBABLE	El evento puede ocurrir en cualquier momento	Al menos 1 vez en los últimos 5 años
3	POSIBLE	El evento puede ocurrir en cualquier momento	Al menos 1 vez en los últimos 2 años
4	PROBABLE	Es viable que el ocurra en algunas circunstancias	Al menos 1 vez en el último 1 año
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Fuente: Subsecretaría de Gestión Institucional, SDG.

12.4. Análisis de impacto

El impacto inicial se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. Los criterios para calificar el impacto en riesgos de soborno dependen del efecto que genera dicho riesgo en las siguientes variables que inciden la gestión de la entidad al momento de la materialización del riesgo, con base en la siguiente tabla:

Tabla 20. Valoración impactos para Riesgos de Soborno

Opción	PREGUNTA Si el riesgo se materializa podría	RESPUESTA	
		SI	NO
1	¿Afecta al grupo de funcionarios del proceso?		X
2	¿Afecta el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afecta el cumplimiento de misión de la Entidad?	X	
4	¿Afecta el cumplimiento de la misión del sector al que pertenece la Entidad?		X
5	¿Genera pérdida de confianza de la entidad, afectando la reputación?	X	
6	¿Genera pérdida de recursos económicos?		X
7	¿Afecta la generación de los productos o la prestación de servicios?	X	
8	¿Da lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Genera pérdida de información de la Entidad?		X
10	¿Genera intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Da lugar a procesos sancionatorios?	X	

12	¿Da lugar a procesos disciplinarios?	X	
13	¿Da lugar a procesos fiscales?		X
14	¿Da lugar a procesos penales	X	
15	¿Genera pérdida de credibilidad del sector?		X
16	¿Ocasiona lesiones físicas o pérdida de vidas humanas?		X
17	¿Afecta la imagen regional?		X
18	¿Afecta la imagen nacional?		X
19	¿Genera daño ambiental?		X
Responder afirmativamente CERO preguntas genera un impacto INSIGNIFICANTE			
Responder afirmativamente UNA a TRES preguntas genera un impacto MENOR			
Responder afirmativamente CUATRO a SEIS preguntas genera un impacto MODERADO		8[2]	
Responder afirmativamente SIETE a ONCE preguntas genera un impacto MAYOR			
Responder afirmativamente DOCE a DIEZ y NUEVE preguntas genera un impacto CATASTRÓFICO			
INSIGNIFICANTE	No genera consecuencias sobre la entidad		
BAJO (MENOR)	Genera consecuencias BAJAS sobre la entidad		
MODERADO	Genera consecuencia MEDIANAS sobre la entidad		
MAYOR	Genera consecuencia ALTAS sobre la entidad		
CATASTRÓFICO	Genera consecuencia DESASTROSAS sobre la entidad		

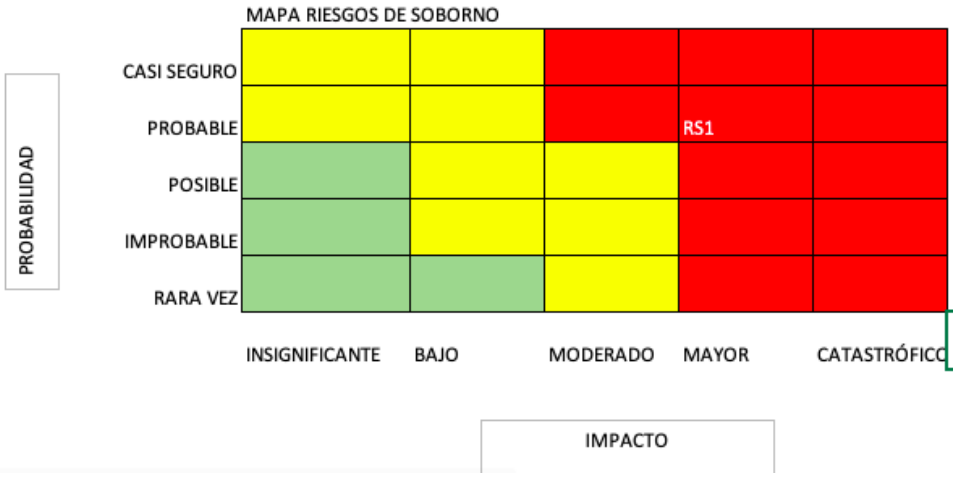
Fuente: Subsecretaría de Gestión Institucional, SDG.

En virtud del impacto en los aspectos indicados, el análisis de impacto se determina teniendo en cuenta los niveles indicados en la tabla anterior, en especial porque se van a analizar muchas situaciones de exposición que van desde nivel insignificante, bajo, moderado, mayor o catastrófico; este orden de ideas, aplican todos los niveles según los impactos que enfrenta la entidad.

Por último, para los riesgos de soborno se aplican todas las probabilidades e impactos descritos, de tal manera que un riesgo se ubica en el Mapa de Riesgos en el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

[2] A manera de ejemplo este resultado corresponde al rango entre Siete y Once, con impacto MAYOR, si por otra parte en la evaluación de probabilidad se determina que el riesgo se ha materializado al menos 1 vez en el último 1 año, se ubica en el Mapa de Riesgo como se observa en la gráfica de calor.

Figura 19. Mapa de riesgos de soborno



Como se observa en la anterior gráfica un riesgo es la combinación de probabilidad e impacto, este primer análisis se denomina RIESGO INHERENTE.

A continuación, se presenta la metodología para obtener el RIESGO RESIDUAL, luego de determinar los controles diseñados, valorar y ejecutar los Controles, dependiente de la solidez de dichos controles para reducir el riesgo inherente a un nivel de menor probabilidad.

12.5. Valoración y diseño de los controles.

Los controles que se describen corresponden al análisis de cada una de las actividades expuestas al soborno, con las evidencias reflejadas en los procedimientos analizados. Los controles descritos tienen el objetivo de responder a las causas que general los riesgos, por lo tanto, existen controles preventivos y correctivos como lista desplegable en la Matriz de Riesgos bajo la denominación CLASE DE CONTROL EXISTENTE, según la experiencia del equipo técnico que realiza el análisis.

Para el diseño de controles, se asumen los parámetros señalados en la versión 5 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2020. En la matriz de riesgos de soborno se aplica la siguiente tabla:

Tabla 21. Valoración de controles.

CONTROLES	**DESCRIPCIÓN DEL CONTROL**	COLUMNA PARA DIGITAR RESPUESTA: Corresponde a los controles reales que se aplican en los procedimientos actuales
	CAUSA QUE ATACA	COLUMNA TIPO LISTA: 1.- Mitiga causa 1, 2.- Mitiga causa 2, 3.- Mitiga causa 3, 4.- Mitiga causa 4, 5.- Mitiga causa 5 o 6.- Mitiga causa 6.
	CLASE DE CONTROL EXISTENTE	COLUMNA TIPO LISTA: Preventivo o Correctivo

Fuente: Subsecretaría de Gestión Institucional, SDG.

Tabla 22. Diseños de Controles.

DISEÑO DE CONTROL	**1. ¿Existe un responsable asignado de la ejecución?**	COLUMNA TIPO LISTA: Si o No
	2. ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	COLUMNA TIPO LISTA: Si o No
	3. ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo en manera oportuna?	COLUMNA TIPO LISTA: Si o No
	4. ¿Las actividades que desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que puedan dar origen al riesgo, ejemplo: Verificar, Validar, Cotejar, Comparar, ¿Revisar?	COLUMNA TIPO LISTA: prevenir o detectar
	5. ¿La fuente de Información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	COLUMNA TIPO LISTA: Si o No
	6. ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	COLUMNA TIPO LISTA: Si o No
	7. ¿Se deja evidencia o rastro de la ejecución del control, que permita cualquier tercero con la evidencia, llegar a la misma conclusión?	COLUMNA TIPO LISTA: Completo, incompleto o no existe
	TOTAL DISEÑO DE CONTROL	se asignan puntos de 0 a 100, lo que genera el rango entre débil, moderado o fuerte.
	RANGO DE CALIFICACIÓN DEL DISEÑO	

Fuente: Subsecretaría de Gestión Institucional, SDG.

En la Matriz de Riesgos en el TOTAL DISEÑO DE CONTROL se hace un balance cuantitativo del análisis de cada control y se asignan puntos de 0 a 100 según corresponda con la fortaleza de los controles, lo anterior genera un RANGO DE CALIFICACIÓN DEL DISEÑO DEL CONTROL como débil, moderado o fuerte.

A continuación, se realiza el análisis de NIVEL DE EJECUCIÓN DEL CONTROL en una lista desplegable con los niveles Siempre, Algunas Veces o No Se Ejecuta, y cada decisión determina el RANGO DE CALIFICACIÓN DE LA EJECUCIÓN, como débil, moderado o fuerte.

Tabla 23. Ejecución del Control

EJECUCIÓN DEL CONTROL	**NIVEL DE EJECUCIÓN DEL CONTROL**	Siempre, algunas veces o no se ejecuta
	RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	Control débil, moderado o fuerte

Fuente: Subsecretaría de Gestión Institucional, SDG.

El siguiente paso es determinar la SOLIDEZ INDIVIDUAL DE CADA CONTROL para lo cual se asocian el RANGO DE CALIFICACIÓN DEL DISEÑO DEL CONTROL con el RANGO DE CALIFICACIÓN DE LA EJECUCIÓN lo que determina si el control es fuerte, moderado o débil.

En el TOTAL SOLIDEZ INDIVIDUAL se determina asignando puntos de cero a 100, según la solidez que genera, la valoración asignada por el equipo evaluador del riesgo.

Tabla 24. Solidez individual de cada control.

SOLIDEZ INDIVIDUAL DE CADA CONTROL	**SOLIDEZ INDIVIDUAL DE CADA CONTROL**	Fuerte, moderado o débil,
	TOTAL SOLIDEZ INDIVIDUAL	De 0 a 100 puntos

Fuente: Subsecretaría de Gestión Institucional, SDG.

Una vez realizada la valoración individual de cada control se hace el análisis de SOLIDEZ DEL CONJUNTO DE CONTROLES (Actividad similar) con un PROMEDIO DE LOS CONTROLES DE RIESGO para los eventos de exposición al riesgo de soborno de las actividades similares analizadas, es decir puede ser débil, moderado o fuerte según corresponda a los promedios de puntos asignados al conjunto de controles.

Tabla 25. Solidez del conjunto de controles

SOLIDEZ CONJUNTO DE CONTROLES (Actividad similar)	**PROMEDIO DE LOS CONTROLES DE RIESGO**	Promedio de riesgos de actividades similares.
	CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	De cero a 100 Puntos puede ser débil, moderado o fuerte

Fuente: Subsecretaría de Gestión Institucional, SDG.

12.6. Niveles de riesgo

Riesgo inherente

El nivel de riesgo inherente se obtiene de la evaluación de Probabilidad por el Impacto que genera el riesgo , así las cosas el riesgo inherente puede ser Insignificante, Menor, Moderado, Mayor o Catastrófico, y la probabilidad Rara Vez, Improbable, Posible, Probable o Casi seguro, Se observa que para cada uno de los roles existe un nivel de impacto y probabilidad, esto significa que para los riesgos de soborno se califica independiente.

Tabla 26. Nivel de riesgo inherente.

Riesgo Inherente	**PROBABILIDAD**	COLUMNA TIPO LISTA: Rara Vez, Improbable, Posible, Probable o Casi seguro
	IMPACTO	COLUMNA define impacto:
	EVALUACIÓN	

Fuente: Subsecretaría de Gestión Institucional, SDG.

Riesgo residual

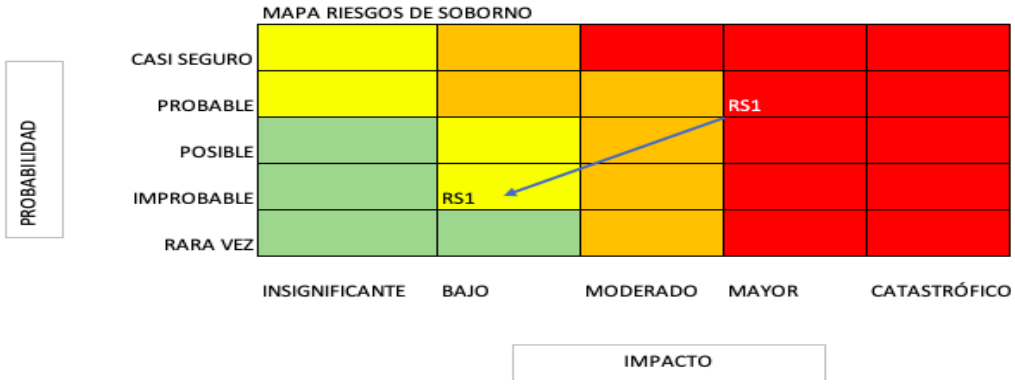
El riesgo inherente se puede reducir en la valoración de probabilidad, más no en el impacto, porque para los riesgos de soborno los impactos son difíciles de controlar y existe cero tolerancia con el Soborno.

Para obtener el RIESGO RESIDUAL, en primera instancia determinan los controles diseñados, la valorar y ejecución de los Controles, dependiendo de la solidez de dichos controles para reducir el riesgo inherente a un nivel de menor probabilidad, como se describe en este manual en al numeral 10.5. Valoración y diseño de los controles.

Una vez que el conjunto de controles se clasifica como fuerte se logra un valor en la CASILLAS QUE MUEVE EN PROBABILIDAD y este valor permite reducir la probabilidad. En este momento nuevamente se hace la evaluación entre la nueva probabilidad y el impacto para determinar el RIESGO RESIDUAL.

En la siguiente gráfica se observa como el riesgo baja de Riesgo Inherente a Riesgo Residual

Figura 20. Ubicación del riesgo residual



12.7. Definición del mapa de calor de riesgos de soborno

Índice Exposición

Para determinar el Mapa de Calor por procesos, se ha establecido tres niveles de exposición con valores de uno (1) para riesgo residual bajo, tres (3) para nivel moderado y cinco (5) para niveles alto y extremo, este índice significa que un riesgo es calificado por su nivel de probabilidad e impacto en esta escala. Al hacer la sumatoria de exposición para cada uno de los procesos y hace una comparación relativa se determina los procesos con exposición baja, media y alta.

Es así como por efecto de la asignación de la exposición general el mapa de calor por procesos, con base en los niveles de exposición relativa para todos y cada uno de los procesos de la entidad; el cálculo en la Matriz de Riesgos de Soborno se ha automatizado para hacer más práctico el uso de la matriz, como se observa en la siguiente tabla:

Tabla 27. Mapa de calor de riesgo de soborno por procesos.

PROCESOS	PUNTAJE CRITICIDAD RIESGO	VALOR RELATIVO	CRITICIDAD POR RIESGO DE SOBORNO	TOTAL RIESGOS
Planeación Institucional	0	0	BAJO	0
Planeación y Gestión Sectorial	0	0	BAJO	0
Gerencia de TIC			MEDIO	
Gestión del Patrimonio Documental	0	0	BAJO	0
Comunicación Estratégica	0	0	BAJO	0
Gerencia del Talento Humano	0	0	BAJO	0
Gestión Corporativa Institucional	0	0	BAJO	0
Control Disciplinario	0	0	BAJO	0
Gestión Jurídica	0	0	BAJO	0
Fomento y protección de los DDHH	0	0	BAJO	0
Convivencia y Diálogo social	0	0	BAJO	0
Relaciones Estratégicas	0	0	BAJO	0
Acompañamiento a la gestión local	0	0	BAJO	0
Inspección, Vigilancia y Control	0	0	BAJO	0
Gestión Pública Territorial Local	0	0	BAJO	0
Gestión del Conocimiento	0	0	BAJO	0

Evaluación Independiente	**0**	**0**	**BAJO**	**0**
Servicio a la ciudadanía	**0**	**0**	**BAJO**	**0**
MÍNIMO VALOR			**TOTAL CANTIDAD RIESGOS**	
MÁXIMO VALOR				

Fuente: Subsecretaría de Gestión Institucional, SDG 2022.

Para los Riesgos de Soborno, el Mapa de Calor se establece por procesos como se observa anteriormente, dado que por la metodología implementada para responder a la norma técnica se hace necesario realizar una debida diligencia detallada, por cada uno de los procedimientos de los procesos, para identificar las ACTIVIDADES SUSCEPTIBLES DE SOBORNO, esto genera un volumen de riesgos por procesos que hacen visualmente alta la cantidad de riesgos en cada uno de los cuadrantes del mapa de riesgos clásico como se observa en la Guía de Riesgos del DAFP.

12.8. Tratamiento del riesgo

La metodología de Gestión de Riesgos de Soborno establecida con base en la Norma Técnica ISO 37001 hace referencia al tratamiento de riesgos calificados en niveles medios o altos, puesto que no se aceptan las prácticas de soborno, por lo tanto a la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este en el logro de los objetivos estratégicos y la relación costo-beneficio de las medidas de tratamiento.

Sin embargo, en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles medio o alto se deberán revisar los controles existentes e implementar el tratamiento de riesgos que sea pertinente. En todos los casos, para los riesgos de soborno la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Tratamiento para aceptar el riesgo

Para los riesgos de soborno el apetito del riesgo de soborno es únicamente el nivel bajo, por lo cual no se aceptan los riesgos en nivel moderado, ni altos, ni extremos. Lo que significa que deben existir planes de tratamiento de riesgos y controles adicionales de segunda línea de defensa para todos los riesgos que se ubican en niveles superiores a bajo; lo anterior significa que la Secretaría Distrital de Gobierno existe cero tolerancia a riegos por encima de bajo.

Tratamiento para evitar el riesgo

Cuando los escenarios de riesgo de soborno identifican riesgos en niveles medios o altos se debería tomar la decisión de evitar el riesgo, para tal efecto se podrá realizar una restructuración de la actividad o un conjunto de actividades, en un procedimiento o documento del sistema de gestión.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es una decisión estratégica, es menos arriesgada y de bajo costo, pero se puede analizar con detalle para no afectar el desarrollo de las actividades de

la entidad y, por lo tanto, hay situaciones donde no es una opción; para estos casos se podrá implementar controles adicionales que sean pertinentes.

Tratamiento para compartir el riesgo

Para los riesgos de soborno cuando es difícil para la entidad reducir el riesgo a un nivel aceptable, el riesgo residual puede ser compartido con otra área funcional de le entidad o con otra parte interesada para gestionarlo en conjunto con más eficacia. Cabe señalar que normalmente no es fácil transferir la responsabilidad de los riesgos de soborno.

Tratamiento para reducir el riesgo

Para los riesgos de soborno el nivel de riesgo debería ser administrado mediante el establecimiento de nuevos controles, de modo que el riesgo residual se pueda reducir a un nivel aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad, pero se debe asumir el impacto del riesgo según sea pertinente.

La SDG debería seleccionar controles apropiados, con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

12.9. Monitoreo de los riesgos de soborno

Los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de soborno y si es el caso ajustar dichos riesgos a las circunstancias. Le corresponde, igualmente, a un profesional de la Subsecretaría de Gestión Institucional por delegación de la persona que ejerce el rol de Oficial de Cumplimiento adelantar el monitoreo (segunda línea de defensa).

La importancia del monitoreo radica en la necesidad de llevar a cabo un seguimiento periódico a la gestión del riesgo de soborno y validar la efectividad de los controles establecidos, teniendo en cuenta que el soborno es, por sus propias características, un delito difícil de detectar.

El monitoreo se realiza en la matriz correspondiente, para tal efecto se debe dejar constancia escrita de los ajustes que se realizan; dicho monitoreo consiste las siguientes actividades:

- Revisar si algún riesgo se ha materializado para verificar si se cumplió el reporte y debida diligencia.
- Revisar cada uno de los controles de primera línea de defensa, para indicar si están vigentes o se están aplicando en debida forma, lo que nos indica la eficacia de todos los controles.
- Revisar la viabilidad de implementar nuevos controles que sean pertinentes para reducir los riesgos clasificados en nivel medio y alto.

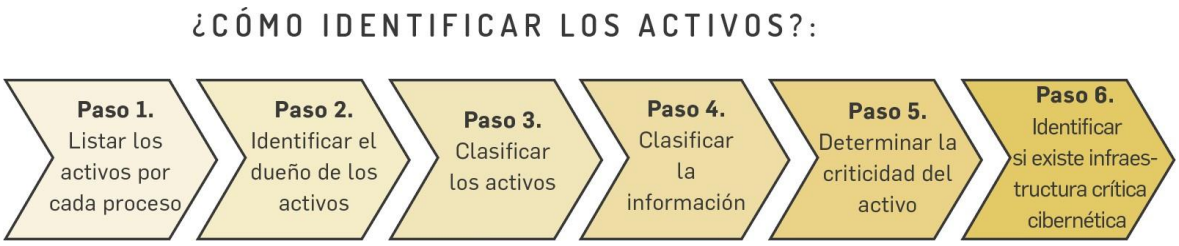
Los monitoreos se realizarán de forma periódica de la siguiente forma:

- Primer monitoreo: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo monitoreo: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer monitoreo: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los veinte (20) primeros días del mes de enero.
- El monitoreo es adelantado por la Subsecretaría de Gestión Institucional y se publicará en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

13. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)3, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Figura 21. Pasos para la identificación de activos



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018

La identificación de los activos de seguridad digital de la información hace parte de la identificación del contexto del proceso, esto con el fin identificar un panorama más acertado de los riesgos de seguridad digital y su calificación en las etapas posteriores del ciclo de gestión del riesgo.

Dado esto, del análisis de los objetivos estratégicos de la entidad, se tiene que un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos digitales 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.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

La SDG posee bases de datos, archivos digitales, servidores web o aplicaciones claves para prestar sus servicios. Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento de cara al ciudadano aumentando así su confianza en el uso del entorno digital.

Para dar cumplimiento a estos lineamientos desde el proceso de "Gerencia de TIC" y "Gestión del Conocimiento" acorde a sus funciones en lo referente a la gestión del riesgo de seguridad digital y buscando dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información y seguridad digital aplica lo establecido en los procedimientos: GCN-P007 "Levantamiento del Catálogo de Componentes de la Información" y GDI-DTI-P004 "Identificación y Valoración de Activos de Información" donde se establecen los lineamientos para la gestión de activos y la valoración de la criticidad de activos. GDI-TIC-F032 Formato identificación, valoración y clasificación de activos de información

Para esta identificación de activos, se tendrá en cuenta la siguiente tipología:

- Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de

confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.

- Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- Intangibles: Aquellos activos inmateriales que otorgan a la Entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el Good Will, entre otros.
- Componentes de red: Medios necesarios para la realizar la conexión de los elementos de hardware y software en una red.
- Instalaciones: Espacio o área asignada para alojar o salvaguardar los datos considerados como activos críticos para la empresa.
- Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

Así mismo, valorar los activos de acuerdo con:

- Confidencialidad

Tabla 28. Confidencialidad

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Fuente: Dirección de Tecnologías e Información, SDG.

- Integridad

Tabla 29. Integridad

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente: Dirección de Tecnologías e Información, SDG.

- Disponibilidad

Tabla 30. Disponibilidad

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Fuente: Dirección de Tecnologías e Información, SDG.

Para determinar las causas de los riesgos de seguridad de la información se diligencia el formato "Matriz mapa de riesgos de seguridad de la información" PLE-PIN-F042, se deben tener en cuenta los siguientes lineamientos:

Para riesgos de seguridad digital, en el componente de causa se deben tener en cuenta los siguientes elementos:

- **Amenaza:** Evento, situación, circunstancia que bajo ciertas condiciones internas (vulnerabilidades) de la SDG tiene el potencial de afectar negativamente un área de impacto de la Entidad. Una amenaza es el peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales.
- **Vulnerabilidad:** Condiciones internas de la SDG relacionadas a defectos, debilidades o ausencias de control que facilitan la materialización de una amenaza.

Se debe tener en cuenta las vulnerabilidades o debilidades de los activos de información que pueden ser aprovechadas por una amenaza (Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización), constituyéndose en fallas.

Identificación de Amenazas: Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas.

- Deliberadas (D),
- fortuito (F)
- ambientales (A).

Tabla 31. Amenazas comunes.

EJEMPLOS DE AMENAZAS COMUNES		
Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D

EJEMPLOS DE AMENAZAS COMUNES		
Tipo	Amenaza	Origen
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de médios de documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Fuente: Dirección de Tecnologías e Información, SDG.

- Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla 32. Fuentes de amenazas humanas

FUENTES DE AMENAZAS HUMANAS		
Fuente de Amenaza	Motivación	Acciones Amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	Piratería
		Ingeniería social
		Intrusión, accesos forzados al sistema
		Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador (por ejemplo, espionaje cibernético)
		Acto fraudulento (por ejemplo, repetición, personificación, interceptación)
		Soborno de la información
		Suplantación de identidad
		Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/terrorismo
		Guerra de la información (warfare)
		Ataques contra el sistema (por ejemplo, negación distribuida del servicio)
		Penetración en el sistema
		Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	Ventaja de defensa
		Ventaja Política
		Explotación económica
		Hurto de información
		Intrusión en la privacidad personal
		Ingeniería social
		Penetración en el sistema
		Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (por ejemplo, error en el ingreso de los datos, error de programación)	Asalto a un empleado
		Chantaje
		Observar información reservada
		Uso inadecuado del computador
		Fraude y hurto
		Soborno de información

FUENTES DE AMENAZAS HUMANAS		
Fuente de Amenaza	Motivación	Acciones Amenazantes
		Ingreso de datos falsos o corruptos
		Interceptación
		Código malicioso (por ejemplo, virus, bomba lógica, troyano)
		Venta de información personal
		Errores en el sistema (bugs)
		Intrusión al sistema
		Sabotaje del sistema
		Acceso no autorizado al sistema

Fuente: Dirección de Tecnologías e Información, SDG.

- Para las vulnerabilidades se debe tener en cuentan la tabla de vulnerabilidades de la norma ISO27001.
- Para los controles de seguridad digital, se deben tener en cuenta los controles establecidos en la norma ISO27001.

14. DOCUMENTOS RELACIONADOS

14.1. Documentos internos

Código	Documento
PLE-PIN-P015	Administración y monitoreo de riesgos de gestión y corrupción
PLE-PIN-P017	Procedimiento Gestión de riesgos de seguridad de la información
GCN-M002	Manual para la gestión de planes de mejoramiento
GCN-P007	Levantamiento del Catálogo de Componentes de la Información
GDI-TIC-P004	Identificación y Valoración de Activos de Información
PLE-PIN-F001	Formato matriz de riesgos por procesos
PLE-PIN-F002	Formato matriz de riesgos de corrupción
PLE-PIN-F035	Formato monitoreo de riesgos
PLE-PIN-F042	Formato matriz de riesgos de seguridad de la información
PLE-PIN-F043	Formato matriz de seguimiento riesgos de corrupción
PLE-PIN-F054	Formato Matriz de riesgos de soborno

14.2. Normatividad Vigente

Norma	Año	Epígrafe	Artículo(s)
Constitución Política de Colombia	1991	En ejercicio de su poder soberano, representado por sus delegatarios a la Asamblea Nacional Constituyente, invocando la protección de Dios, y con el fin de fortalecer la unidad de la Nación y asegurar a sus integrantes la vida, la convivencia, el trabajo, la justicia, la igualdad, el conocimiento, la libertad y la paz, dentro de un marco jurídico, democrático y participativo que garantice un orden político, económico y social justo, y comprometido a impulsar la integración de la comunidad latinoamericana, decreta, sanciona y promulga.	209 y 269
Ley 489	1998	Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones	Todos
Ley 1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.	Todos
Decreto 2145	1999	Por la cual se dictan normas sobre el Sistema Nacional de control interno de las entidades y organismos de la administración pública del orden nacional y territorial y se dictan otras disposiciones. Modificado parcialmente por el Decreto 2593 del 2000.	Todos
Decreto 1537	2001	Reglamenta parcialmente la Ley 87 de 1993. Estableció que todas las entidades de la Administración Pública deben contar con una	Todos

Norma	Año	Epígrafe	Artículo(s)
		política de administración de riesgos.	
Decreto 371	2010	Por el cual se establecen lineamientos para preservar y fortalecer la transparencia y para la prevención de la corrupción en las Entidades y Organismos del Distrito Capital.	Todos
Decreto 2641	2012	Por el cual se reglamentan los artículos 73 y 76 de la ley 1474 de 2011.	Todos
Decreto 1499	2017	Por medio del cual se modifica el Decreto número 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.	Todos
Resolución 0219	2018	Por la cual se reglamenta el funcionamiento del Comité Institucional de Coordinación de Control Interno de la Secretaría Distrital de Gobierno y se deroga la resolución No 1921 del 2016	Todos
Resolución 0783	2018	Por la cual se crea el Comité Institucional de Gestión y Desempeño y se dictas otras disposiciones.	Todos
Resolución 236	2019	Modificación Resolución 783 de 2018	Todos

14.3. Documentos externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Guía GTC 104. Gestión del Riesgo Ambiental. Principios y Proceso	2009	ICONTEC	Digital
CONPES 3714 Del riesgo previsible en el marco de la política de contratación pública	2011	Consejo nacional de política económica y social CONPES	https://www.colombiacompra.gov.co/sites/default/files/normativas/conpes3714.pdf
NTC GTC 137 Gestión del Riesgo Vocabulario	2011	ICONTEC	Digital

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
NTC ISO 31000. Gestión del Riesgo. Principios y directrices	2011	ICONTEC	Digital
Guía Técnica Colombiana GTC 45	2012	ICONTEC	Digital
MODELO DE TRES LINEAS DE DEFENSA proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.	2013	Instituto de Auditores Internos, publicó el documento "Leveraging COSO Across the Three Lines of Defense"	Digital
NTC IEC / ISO 31010 Norma Técnica Colombiana Gestión de Riesgos. Técnicas de Valoración del Riesgo	2013	ICONTEC	Digital
NTC ISO 27001 Norma Técnica Colombiana que establece los requisitos de un Sistema de Gestión de Seguridad Digital de la Información.	2013	ICONTEC	Digital
MECI 2014 Manual técnico del modelo estándar de control interno para el Estado Colombiano	2014	Departamento Administrativo de la Función Pública	Digital
NTC ISO 14001 Norma Técnica Colombiana	2015	ICONTEC	Digital
MODELO COSO ERM La Gestión Integral de Riesgos (ERM) forma parte de las buenas prácticas de gestión empresarial y es un proceso que permite tratar eficazmente la incertidumbre, identificando riesgos y oportunidades, y optimizando la capacidad de generar valor.	2017	Committee of Sponsoring Organizations of the Treadway Commission Instituto de Auditores internos de España. Organismo de reconocimiento internacional donde se establecen los marcos reguladores básicos de riesgo y cumplimiento en temas de control interno.	Digital
NTC ISO 37001	2017	Sistemas de gestión antisoborno	Digital