
GUIA INTEGRAL PARA LA
GESTIÓN DEL RIESGO
SECRETARÍA DISTRITAL DE
SEGURIDAD, CONVIVENCIA Y JUSTICIA

TABLA DE CONTENIDO

1 INTRODUCCIÓN

La Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) adopta la presente guía como instrumento metodológico para orientar la gestión integral del riesgo en la entidad, en coherencia con la Política Integral de Gestión del Riesgo y los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP).

Esta guía tiene como propósito facilitar la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos en los diferentes procesos institucionales, incorporando de manera transversal los riesgos de gestión, estratégicos, operativos, financieros, tecnológicos, de seguridad de la información y, especialmente, los riesgos de integridad pública, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).

El enfoque adoptado reconoce que la gestión del riesgo no es un ejercicio aislado, sino una práctica continua que hace parte de la toma de decisiones y del desarrollo normal de las actividades institucionales. En este sentido, todos los servidores públicos y contratistas que participan en los procesos tienen un rol activo en la identificación y control de los riesgos, desde su conocimiento del contexto y de la operación.

Asimismo, la guía articula el modelo de las líneas de defensa, definiendo responsabilidades claras entre la primera línea (gestión), la segunda línea (orientación y seguimiento) y la tercera línea (aseguramiento independiente), garantizando la trazabilidad de la información, la adecuada segregación de funciones y la generación de valor a través del control.

De manera particular, se incorpora el tratamiento diferencial para los riesgos de integridad pública, frente a los cuales la entidad adopta un enfoque de apetito cero. Esto implica que no se admite su aceptación pasiva, sino la aplicación permanente de controles preventivos reforzados, monitoreo continuo y mecanismos estrictos de seguimiento, sin desconocer que dichos riesgos pueden materializarse y, por tanto, deben gestionarse de manera oportuna.

Finalmente, la guía establece criterios homogéneos para la documentación de los riesgos, la definición de controles, la construcción de indicadores y la validación de evidencias, con el fin de fortalecer la calidad de la información y facilitar su seguimiento por parte de la segunda línea de defensa y los órganos de control.

Para realizar una adecuada integración y adopción de la guía para la gestión integral del riesgo del DAFP versión 7, se debe contemplar la estructura general identificando el marco conceptual, estructura, herramientas e implementación establecidas en el documento, como se representa en la siguiente imagen.

GUÍA PARA LA GESTIÓN INTEGRAL DEL RIESGO

(Función Pública – Versión 7, 2025)

1. ENFOQUE GENERAL Y ACTUALIZACIONES DE LA V7

- Basada en ISO 31000 e incorpora COSO-ERM (2017).
- Articulada con MIPG y MECI (líneas de aseguramiento).
- Integra políticas públicas: Transparencia e Integridad, Gobierno Digital (TI), Salud, entre otras.
- Incluye SIGRIP y el enfoque de riesgos fiscales, de corrupción y de seguridad de la información.

2. ESTRUCTURA PRINCIPAL DE LA GUÍA (CAPÍTULOS I-VIII)

- Cap. I — Alineación estratégica con MIPG/MECI: políticas, gobernanza y valor público.
- Cap. II — Aspectos clave previos: modelo por procesos, niveles de madurez, política y apetito de riesgo.
- Cap. III — Riesgos generales de la gestión: identificación, probabilidad, impacto, severidad, controles y mapa integral.
- Cap. IV — Gestión preventiva de riesgos fiscales: control fiscal interno y catálogo de puntos de riesgo.
- Cap. V — Riesgos de seguridad de la información: activos, clasificación, amenazas/vulnerabilidades y valoración.
- Cap. VI — SIGRIP (Integridad pública): soborno, fraude, conflicto de intereses, LA/FT/FP y función de cumplimiento.
- Cap. VII — Articulación para entidades vigiladas por Supersalud (sector salud).
- Cap. VIII — Seguimiento, monitoreo e indicadores (KRI/KPI) y mejora continua.

3. CAJA DE HERRAMIENTAS Y ANEXOS

- Anexo 1: Matriz mapa de riesgos parametrizada.
- Anexo 2: Glosario de términos y definiciones.
- Anexo 3: Catálogo indicativo de puntos de riesgo fiscal.
- Anexo 4: Matriz de madurez (autoevaluación COSO-ERM).
- Anexo 5: Matriz de riesgos de seguridad de la información.

4. ARTICULACIÓN INSTITUCIONAL Y ACTORES CLAVE

- Alta Dirección: define política, apetito y asigna recursos.
- Comité Institucional de Gestión y Desempeño: aprueba/monitorea política y riesgos estratégicos.
- Comité de Coordinación de Control Interno: alcance de auditorías y mejoras del sistema.
- Oficina de Control Interno (3ª línea): evaluación de controles y recomendaciones.
- Líderes de proceso (1ª línea) y gestores de riesgo (opcional, 2ª línea): gestión diaria.

5. ESQUEMA DE DESPLIEGUE METODOLÓGICO

- Identificación del riesgo.
- Valoración (probabilidad × impacto = severidad).
- Diseño y valoración de controles (preventivos, detectivos y correctivos).
- Definición del tratamiento y cálculo del riesgo residual.
- Consolidación del Mapa de Riesgos Integral.
- Seguimiento con KRI/KPI y mejora continua (MECI).

Secretaría Distrital de Seguridad, Convivencia y Justicia – Alcaldía Mayor de Bogotá D.C.
Elaboró: Juan Carlos Cepeda Moncada

2 OBJETIVO

Orientar la gestión integral del riesgo de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, suministrando lineamientos metodológicos para identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, institucionales y de proceso.

La guía desarrolla la Política Integral de Gestión del Riesgo V4 y se articula con la Guía DAFP V7, el MIPG, el MECI y el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP; Incluye criterios para la gestión de riesgos de gestión, estratégicos, fiscales, integridad pública, emergentes, así como la gestión de oportunidades institucionales.

3 ALCANCE

Aplica a todos los procesos del modelo de operación por procesos de la SDSCJ, desde el análisis del contexto y el conocimiento del proceso hasta la identificación, valoración, tratamiento, monitoreo, seguimiento, reporte de materializaciones y mejora continua.

Los riesgos no relacionados en la presente guía, conservan su tratamiento diferencial y especializado, en armonía con la política y los manuales y/o documentos que operativizan cada tipología.

4 AMBITO DE APLICACIÓN

Aplica a todas las dependencias, sedes, procesos, programas, proyectos, servidores públicos y contratistas de la SDSCJ, en niveles estratégicos, misionales, de apoyo y de evaluación.

5 NORMATIVIDAD ASOCIADA

- Guía para la Gestión Integral del Riesgo en Entidades Públicas – DAFP, Versión 7 (2025).
- Decreto 1122 de 2024 y su anexo técnico sobre PTEP.
- Ley 2195 de 2022
- Decreto 1499 de 2017 – MIPG
- Ley 87 de 1993 y Decreto 648 de 2017.
- Normas ISO aplicables según la tipología de riesgo y el alcance institucional.

La normatividad asociada se encuentra en el portal del Modelo Integrado de Planeación y Gestión -MIPG-. Ver Normas del proceso en https://portalmipg.scj.gov.co

6 DOCUMENTOS ASOCIADOS

- F-DE-1379 Matriz de Contexto Estratégico
- F-FI-1385 Matriz de Riesgos de Seguridad de la Información
- F-FI-1383 Matriz de Identificación Calificación y Seguimiento de Oportunidades

7 GLOSARIO

Acción Correctiva: Acción tomada para eliminar y/o mitigar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

Acción Preventiva: Acción tomada para eliminar la(s) causa(s) de una no conformidad u otra situación potencial no deseable.

Activo (Documento CONPES 3854 de 2016, pág.56): Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada Entidad, órgano u organismo.

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

Activo cibernético: En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Administración del riesgo: Es la capacidad que tiene la organización para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Documento CONPES 3854).

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2018).

Alta Dirección: Máximo nivel jerárquico y de toma de decisiones dentro de la organización, que para la entidad es el Secretario/a de Seguridad.

Apetito de riesgo:Nivel de riesgo que una entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe gestionar.

Ataque cibernético: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

Beneficiario Final: Persona natural que, en última instancia, posee, controla o se beneficia directa o indirectamente de una persona jurídica o de una operación. Su identificación permite conocer la estructura real de propiedad y control, y constituye un elemento clave para la prevención de riesgos asociados a lavado de activos, financiación del terrorismo y corrupción.

CCOC: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

Capacidad de riesgo: Nivel máximo de exposición que la entidad puede soportar sin comprometer sus objetivos; máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. (relacionado con la solvencia y liquidez).

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un 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: Situación que puede determinar porqué ocurrir un evento no deseado. Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Comisión de Coordinación Interinstitucional para el control del lavado de activos (CCICLA): La Comisión de Coordinación Interinstitucional para el Control del Lavado de Activos, CCICLA, es el organismo consultivo del Gobierno Nacional y ente coordinador de las acciones que desarrolla el Estado Colombiano para combatir el lavado de activos y la financiación del terrorismo.

Componentes de red: Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.

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

Confidencialidad: Propiedad de la información que la hace no disponible, es decir divulgada a individuos, Entidades o procesos no autorizados.

Control: Es toda medida, acción, política, procedimiento o mecanismo diseñado e implementado por la entidad para modificar el riesgo. Su propósito fundamental es aumentar la probabilidad de alcanzar los objetivos institucionales, ya sea mediante la reducción de la probabilidad de ocurrencia del evento o la mitigación de su impacto negativo.

Control Correctivo: Conjunto de medidas, acciones o mecanismos diseñados para subsanar las consecuencias de un evento de riesgo una vez este se ha materializado. Su objetivo principal es restablecer la normalidad de la operación, corregir las desviaciones detectadas y evitar la recurrencia del evento mediante el ajuste de los controles preventivos o detectivos que fallaron.

Control Detectivo: Es aquel diseñado para identificar y alertar sobre la ocurrencia de un evento de riesgo, error o irregularidad en el momento en que sucede o poco después de su ejecución. A diferencia del preventivo, este control actúa cuando la causa ya se ha manifestado, permitiendo a la entidad reaccionar de manera oportuna para mitigar el impacto o activar medidas correctivas.

Control Preventivo: Es toda medida, política o procedimiento diseñado para intervenir sobre las causas que originan un riesgo, con el fin de evitar su ocurrencia. Su propósito es actuar de manera proactiva antes de que el evento se materialice, minimizando la probabilidad ocurrencia. Al operar en la fase inicial del ciclo del riesgo, se considera la barrera más eficiente para asegurar que los objetivos institucionales se alcancen dentro de los niveles de tolerancia definidos.

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. Se manifiesta a través del abuso de una posición de confianza o autoridad para obtener ventajas ilícitas, ya sea para sí mismo o para terceros, comprometiendo la integridad, la transparencia y el cumplimiento de los fines esenciales del Estado.

Debida Diligencia: Conjunto de procedimientos y controles que implementa la entidad para conocer, verificar y evaluar a sus contrapartes (personas naturales o jurídicas), con el fin de prevenir riesgos asociados al SIGRIP (corrupción, lavado de activos, financiación del terrorismo y otras conductas que afecten la integridad pública). Incluye la verificación en listas vinculantes y restrictivas, la validación de información y el análisis del nivel de riesgo de la contraparte.

Debida Diligencia Reforzada: Aplicación de medidas adicionales de verificación y análisis cuando se identifican factores de mayor riesgo en una contraparte, tales como alertas en listas restrictivas, operaciones inusuales o condiciones atípicas. Implica un

mayor nivel de profundidad en la validación de información, el análisis de contexto y la adopción de controles adicionales antes de la toma de decisiones.

Delito: Conducta atípica, antijurídica y culpable que transgrede el ordenamiento legal vigente; es la materialización de un riesgo legal y de cumplimiento que afecta la legitimidad de la institución

Delito fuente: Evento que genera la riqueza ilegal, los cuales se buscan introducir en el sistema económico legal para darles apariencia de legalidad. Proceso posterior de ocultar el origen ilegal de dineros, para que parezca legal en las cuentas de la entidad, del sistema económico, productivo y/o financiero a través de terceros.

Detección: Cuando se determina la ocurrencia de posibles operaciones de lavado de activos o financiación del terrorismo.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por la Entidad.

Efectos: Constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la Entidad, generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y vulneración de los derechos de las personas privadas de la libertad, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Evaluación del Riesgo: Proceso integral que consiste en comparar los resultados del análisis del riesgo con los criterios de riesgo establecidos, con el fin de determinar si el riesgo y/o su magnitud son aceptables o tolerables para la entidad; permite priorizar los riesgos identificados, definiendo cuáles requieren un tratamiento inmediato y cuáles pueden ser monitoreados bajo los controles actuales.

Factores de Riesgo: Fuente, circunstancia o elemento, interno o externo, que tiene la capacidad de generar o incrementar la probabilidad de que un riesgo se materialice; "agentes generadores" que deben ser identificados y monitoreados para entender por qué y cómo podría ocurrir un evento que afecte los objetivos institucionales.

Función de cumplimiento: Rol de segunda línea encargado del liderazgo técnico del SIGRIP y del componente de integridad pública.

Hardware: Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información

ICC: Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grabe impacto sobre los servicios esenciales.

Impacto: Son las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Datos almacenados en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.

Intangible: Se consideran 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

Integridad Pública: Categoría que agrupa riesgos de corrupción, soborno, fraude, conflicto de interés y LA/FT.

Lavado de Activos (LA): Proceso que busca ocultar el rastro documental y el origen real de dineros obtenidos mediante delitos fuente. Riesgo multidimensional de que la entidad sea utilizada como instrumento para canalizar recursos de origen ilícito o para dar apariencia de legalidad a bienes provenientes de actividades delictivas

Línea estratégica: Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno.

Listas Restrictivas (o de control): Conjunto de bases de datos de carácter nacional o internacional que contienen información sobre personas naturales o jurídicas que registran antecedentes, investigaciones, sanciones no vinculantes o alertas asociadas a posibles conductas relacionadas con corrupción, lavado de activos, financiación del terrorismo u otros riesgos de integridad.

La consulta de estas listas constituye una práctica de debida diligencia orientada a la prevención y gestión del riesgo, permitiendo identificar señales de alerta que puedan afectar la toma de decisiones institucional. Su uso no implica, por sí mismo, una prohibición legal automática, pero sí exige la aplicación de análisis reforzados y controles adicionales: RNMC, Policía, UIAF, OFAC, son algunas.

Lista Vinculante: Base de datos cuya consulta y aplicación es obligatoria por ley y tratados internacionales suscritos por Colombia. No admite interpretación ni análisis de riesgo: si una persona o entidad aparece aquí, existe un impedimento legal absoluto para contratar o mantener vínculos, tales como: antecedentes disciplinarios, Boletín de responsables fiscales, lista de Sanciones del Consejo de Seguridad de la ONU

Mapa de Riesgos: Herramienta de gestión estructurada de los riesgos identificados en la entidad, organizados según su nivel de probabilidad e impacto, que permite su análisis, priorización y gestión, en el marco del cumplimiento de los objetivos institucionales y los lineamientos del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP)..

Mitigación del Riesgo: Estrategia mediante la cual la SDSCJ adopta medidas orientadas a reducir la probabilidad de ocurrencia y/o el impacto de un riesgo, con el fin de mantenerlo dentro de niveles aceptables. Estas medidas se materializan a través de la implementación o fortalecimiento de controles preventivos, detectivos y correctivos, así como de acciones específicas que permitan disminuir la exposición al riesgo..

MSPI: Modelo de Seguridad y Privacidad de la Información

Monitoreo del Riesgo: Proceso continuo mediante el cual se observa el comportamiento de los riesgos y la efectividad de los controles en el tiempo. Este proceso permite identificar desviaciones, debilidades en los controles y la aparición de nuevos riesgos, facilitando la toma de decisiones y la implementación de acciones de mejora.

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

Operación inusual: Transacción, actividad o comportamiento que se aparta del patrón habitual o esperado de una persona natural o jurídica, de acuerdo con su perfil, actividad económica o histórico de comportamiento. No necesariamente implica la existencia de una actividad ilícita, pero genera una señal de alerta que requiere análisis para determinar su justificación.

Operación Sospechosa: Transacción, actividad o comportamiento que, luego de ser analizado, no cuenta con una justificación razonable o presenta indicios de posible relación con actividades ilícitas, como el lavado de activos, la financiación del terrorismo, fraude o la corrupción. A diferencia de la operación inusual, la operación sospechosa implica un nivel de alerta mayor, que puede dar lugar a la adopción de medidas internas y, cuando corresponda, al reporte ante las autoridades competentes.

Personas Públicamente Expuestas (PEP): Personas naturales que, por razón de su cargo, función o reconocimiento público, administran recursos públicos, ejercen funciones públicas o tienen un nivel significativo de exposición e influencia, lo que las hace más susceptibles a riesgos asociados al SIGRIP. Incluye tanto a personas que actualmente ocupan cargos públicos como a quienes los hayan ejercido en el pasado, así como a sus familiares y asociados cercanos, según la normativa vigente (Ley 2195 de 2022, Decreto 830 de 2021 y recomendaciones del GAFI).

Política de Administración del Riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000

Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.

Primera Línea de Defensa: Instancia de control conformada por los líderes de proceso, responsables operativos, servidores y contratistas que ejecutan las actividades de la entidad, quienes tienen la responsabilidad directa de identificar, gestionar, controlar y reportar los riesgos en el desarrollo de sus funciones. Son los responsables de implementar los controles, ejecutar las acciones de tratamiento y asegurar que la gestión del riesgo esté integrada en la operación diaria.

Probabilidad: Medida de la posibilidad de que un riesgo se materialice, considerando la frecuencia o la posibilidad de ocurrencia de un evento en un periodo determinado, de acuerdo con las condiciones del entorno y los factores que lo originan.

Programa de Transparencia y Ética Pública (PTEP): Instrumento de gestión adoptado por las entidades públicas en cumplimiento de la Ley 2195 de 2022, que integra medidas para la prevención, detección y gestión de riesgos de corrupción y de integridad pública. El PTEP articula la gestión de riesgos bajo el enfoque del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), incorporando dentro de su alcance riesgos asociados a corrupción, soborno, fraude, conflicto de intereses y LA/FT/FP.

Reporte de Operaciones Sospechosa (ROS): Mecanismo mediante el cual se informa a la Unidad de Información y Análisis Financiero (UIAF) sobre transacciones, actividades o comportamientos que, tras un análisis, no cuentan con justificación económica o legal aparente, o presentan indicios de posible relación con actividades ilícitas como el lavado de activos o la financiación del terrorismo; este reporte debe realizarse de manera oportuna, confidencial y conforme a los lineamientos establecidos por la autoridad competente.

Reporte de Operaciones Inusuales (ROI): Registro interno mediante el cual la entidad documenta y analiza aquellas transacciones, actividades o comportamientos que se apartan del perfil o patrón habitual de una contraparte. Su propósito es dejar evidencia del análisis realizado, permitiendo determinar si la operación cuenta con justificación razonable o si debe escalarse como una operación sospechosa para su eventual reporte ante la Unidad de Información y Análisis Financiero (UIAF).

Riesgo: Evento o condición incierta; efecto de la incertidumbre sobre el cumplimiento de los objetivos institucionales. Posibilidad de que ocurra un evento (interno o externo) que afecte negativamente (o positivamente) la ejecución de los procesos, la prestación del servicio o el logro de las metas del Estado.

Riesgo de Corrupción: Posibilidad de que el poder sea utilizado, ya sea por acción u omisión, para desviar la gestión pública en beneficio privado.

Riesgo de Conflicto de Interés: Posibilidad de que los intereses personales, familiares, económicos o de cualquier otra índole de un servidor público interfieran, o puedan interferir, en el ejercicio objetivo, imparcial y transparente de sus funciones, afectando la toma de decisiones en la entidad.

Riesgos de Fraude: Posibilidad de que, mediante engaño, manipulación o alteración intencional de información, se obtenga un beneficio indebido o se cause un detrimento a los recursos, procesos o resultados de la entidad, afectando la transparencia y confiabilidad de la gestión pública.

Riesgo de Soborno: Posibilidad de que un servidor público o un tercero ofrezca, solicite, entregue o reciba beneficios indebidos (económicos o no), con el propósito de influir en una decisión, actuación o resultado dentro de la entidad, vulnerando los principios de legalidad, transparencia e imparcialidad.

Riesgo de Gestión: Posibilidad de que la gestión de la SDSCJ no logre sus objetivos o no cumpla con las metas establecidas, debido a deficiencias, errores, fallas u omisiones en los procesos, procedimientos, controles, o en la administración de los recursos.

Riesgo de Lavado de Activos y Financiación del Terrorismo – LA/FT: Posibilidad de que la SDSCJ sea utilizada, de manera directa o indirecta, para dar apariencia de legalidad a recursos provenientes de actividades ilícitas (lavado de activos) o para canalizar recursos destinados a la financiación del terrorismo, afectando el cumplimiento de sus objetivos y generando impactos legales, reputacionales, operativos y de integridad.

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 Fiscal: Posibilidad de que, por acción u omisión, se genere un daño al patrimonio público, como consecuencia de una gestión inadecuada, ineficiente, antieconómica o contraria a la normativa vigente en el manejo de los recursos públicos; puede derivarse de decisiones, procesos o actuaciones que afecten la correcta administración de los recursos, dando lugar a posibles responsabilidades fiscales.

Riesgo inherente: Nivel de riesgo al que está expuesta una actividad, proceso u operación antes de la implementación de controles, considerando únicamente sus características propias y los factores internos y externos que lo afectan.

Riesgo Residual: Nivel de riesgo que permanece después de la implementación y aplicación de controles, considerando la efectividad de los mismos para reducir la probabilidad de ocurrencia y/o el impacto del riesgo.

Seguimiento del Riesgo: Verificación puntual y estructurada del cumplimiento de las acciones definidas en los planes de tratamiento del riesgo, es periódico (mensual, trimestral, cuatrimestral), evalúa si las acciones se ejecutaron, y valida evidencias

Sistema de Gestión de Seguridad de la Información - SGSI: Es el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una Entidad, en la búsqueda de proteger sus activos de información esenciales de acuerdo con lo definido en la ISO/IEC 27000.

Segunda Línea de Defensa: Nivel de control encargado de orientar, acompañar y realizar seguimiento a la gestión del riesgo; función técnica responsable de establecer las políticas, metodologías y herramientas para que la operación se mantenga bajo control, además de supervisar y monitorear que la Primera Línea de Defensa (los líderes de proceso) identifique y gestione sus riesgos de manera efectiva..

Servicios: (Digital) Servicio brindado por parte de la Entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).

Servicios Esenciales: Son los necesarios para el mantenimiento de las funciones sociales básicas la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del estado y las administraciones públicas.

Software: Informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades

Tabla de Retención Documental -TRD: Es el listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos, es decir se considera como el Instrumento que permite establecer cuáles son los documentos de una Entidad, su necesidad e importancia en términos de tiempo de conservación y preservación y que debe hacerse con ellos una vez finalice su vigencia o utilidad.

Tercera línea de defensa: Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera línea y la segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno o Auditoría Interna.

Tolerancia del riesgo: nivel de variación aceptable que la entidad está dispuesta a permitir en el logro de un objetivo específico; medida operativa y detallada que define los límites máximos y mínimos de desviación permitidos en la ejecución de los procesos y el desempeño de los controles.

Tratamiento al riesgo: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

UIAF: Unidad de Información y Análisis Financiero es un organismo de inteligencia económica y financiera que centraliza, sistematiza y analiza la información suministrada por las Entidades reportantes y fuentes abiertas, para prevenir y detectar posibles operaciones de lavado de activos, sus delitos fuente, y la financiación del terrorismo.

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

8 DESCRIPCIÓN

Los tipos de riesgo a gestionar en la presente Guia de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ corresponden a los mencionados en Política de Administración de Riesgos:

- Riesgos Estratégicos
- Riesgos de Gestión
- Riesgos de Integridad Pública
- Riesgos de Seguridad de la Información
- Riesgos Fiscales
- Gestión de Oportunidades.

Los riesgos de SSST, Ambientales, y aquellos que correspondan a la obligatoriedad de la SDSCJ, y que no estén tratados en la presente Guia, deberán contar con documentos independientes

9 METODOLOGIA A IMPLEMENTAR

La Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, complementando la metodología desarrollada por el Departamento Administrativo de la Función Pública, realiza un análisis inicial validando el estado de la estructura de riesgos y su gestión en la Entidad al cierre de cada año, esta actividad se desarrolla durante el primer trimestre posterior al cierre del año. Lo anterior se dinamiza con la aplicación de la Metodología para la Administración de Riesgos:

Ilustración 1. Metodología para la Administración de Riesgos
Fuente: Adaptado de la Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

10 ROLES, RESPONSABILIDADES, COORDINACIÓN Y ARTICULACIÓN

En cumplimiento de la normatividad proferida para la implementación del Modelo Integrado de Planeación y Gestión - MIPG en las entidades de la Administración Distrital y las disposiciones del Decreto 1499 de 2017, así como las disposiciones del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017 que reglamenta el funcionamiento del Comité Institucional de Coordinación de Control Interno para la adecuada gestión del riesgo. Las responsabilidades para la gestión integral del riesgo se definen conforme al Esquema de Líneas:

Línea Estratégica (Alta Dirección y Comités): Ejercen la supervisión; son responsables de aprobar la Política Integral para la Gestión del Riesgo, definir el apetito al riesgo , asignar los recursos y analizar los riesgos críticos para la toma de decisiones estratégicas.

Primera Línea (Líderes de Proceso y Servidores): Son los responsables primarios de gestionar los riesgos inherentes a sus procesos y actividades diarias. Deben identificar, evaluar, controlar y reportar sus riesgos.

Segunda Línea (Oficina de Planeación, Gerencia de Riesgos o quien haga sus veces): Diseña la metodología, capacita, asesora y acompaña a la primera línea. Consolida el mapa de riesgos institucional, monitorea los riesgos críticos y analiza el estado de madurez de la gestión.

- **Tercera Línea (Oficina de Control Interno / Auditoría Interna):** Provee aseguramiento y asesoría independiente sobre la efectividad de la gestión de riesgos y los controles implementados en la primera y segunda línea.

Esquema de Líneas de Defensa SDSCJ			
Líneas de Defensa	**Responsable**	**Rol Principal**	**Responsabilidad**
Estratégica	Alta Dirección	Definir, emitir, revisar, validar, supervisar y evaluar el cumplimiento de la presente Política, considerando su aplicación, cambios en el entorno y las	**Establecer y gestionar,** el nivel de apetito, tolerancia y capacidad de riesgo institucional provisto.
			Asegurar el establecimiento de condiciones mínimas para el ambiente de control, incluyendo la cultura organizacional de integridad, el fortalecimiento de capacidades institucionales y el fomento del autocontrol en todos los niveles.

Esquema de Líneas de Defensa SDSCJ			
Líneas de Defensa	**Responsable**	**Rol Principal**	**Responsabilidad**
	Comité Institucional de Gestión y Desempeño	dificultades para su desarrollo.	**Analizar** la gestión del riesgo y aplicar las mejoras.
	Comité Institucional de		**Articular el sistema de control interno** con las tres líneas de defensa.
			Monitorear la operación del sistema de líneas de defensa en particular la operación y articulación de la línea estratégica, asegurando que los roles de gestión de riesgos asignados a cada línea sean ejecutados y que se mantenga su interacción efectiva.

Esquema de Líneas de Defensa SDSCJ			
Líneas de Defensa	**Responsable**	**Rol Principal**	**Responsabilidad**
	Coordinación de Control Interno		**Corresponde al Comité de Control Interno** aprobar y en caso de ser pertinente, modificar la Política de Administración del Riesgo, en cumplimiento a la resolución 215 de 2017.
			Debe asegurar 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.
Primera Línea de Defensa	Subsecretarios, Jefes de Oficina, funcionarios y contratistas que efectúan las actividades que permiten el cumplimiento del objetivo de los procesos y por ende de la entidad.	Identificar, evaluar, controlar y mitigar los riesgos mediante el autocontrol, como mecanismo esencial del SCI.	**Implementar la presente Política** para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.
			Garantizar el monitoreo y revisión periódica de todos los tipos de riesgos de su proceso.
			Coordinar gestión con la Segunda Línea defensa para realizar ajustes sobre los riesgos, para calificación de controles o según sea requerido.
			Reportar la materialización de los riesgos a la Segunda y Tercera línea de Defensa
			Dar cumplimiento al reporte y cargue de evidencias en los repositorios de información destinado por la OAP en los tiempos establecidos.

Esquema de Líneas de Defensa SDSCJ			
Líneas de Defensa	**Responsable**	**Rol Principal**	**Responsabilidad**
			El Gestor de Riesgosserá desempeñado por el Líder Operativo de cada proceso.
Segunda Línea de Defensa	Oficina Asesora de Planeación	Ejecutar la consolidación de la gestión del riesgo estratégico, de integridad pública, así como la difusión y asesoría de la presente metodología, junto al tratamiento de los riesgos identificados en todos los niveles de la Entidad, de tal forma que se asegure su implementación. Desarrollar las funciones de gestor de cumplimiento del SIGRIP	**Capacita, acompaña, genera recomendaciones** a la primera línea con base en los lineamientos definidos.
			Consolidar el Mapa de riesgos (proceso, corrupción (incluye LA/FT), estratégicos, gestión de oportunidades) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional.
			Hacer seguimiento a los controles establecidos por la primera línea de defensa acorde con la información suministrada.
			Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.
			Trabajar coordinadamente con la Oficina de Control Interno, en el fortalecimiento del Sistema de Control Interno.
			Elaborar informes de seguimiento a riesgos según periodicidad establecida.
			Socializar y divulgar en el Comité de Gestión y Desempeño Institucional los resultados de los Informes de Seguimiento y Evaluación de los riesgos elaborados por la Oficina Asesora de Planeación y la Oficina de Control Interno, con el fin de facilitar la toma de decisiones orientadas al fortalecimiento de la gestión del riesgo en la entidad.
	Dirección de Tecnologías y Sistemas de la Información	Consolidar la información de la gestión del riesgo de seguridad de la información, así como la difusión y asesoría de la presente metodología, junto	**Capacita, acompaña, genera recomendaciones** con base a los lineamientos definidos.

Esquema de Líneas de Defensa SDSCJ			
Líneas de Defensa	**Responsable**	**Rol Principal**	**Responsabilidad**
		al tratamiento de los riesgos identificados en todos los niveles de la Entidad, de tal forma que se asegure su implementación.	
	Responsable de Seguridad de la Información	En concordancia con lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones y en la Política de Seguridad y Privacidad de la Información, la SDSCJ delega la responsabilidad de gestionar los riesgos de seguridad de la información al encargado.	**Gestionar los Riesgos de Seguridad de la Información** (identificación, análisis, formalización, evaluación y tratamiento).
			Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
			Apoyar en el seguimiento al tratamiento de los riesgos definidos.
			Presentar a la mesa técnica de seguridad digital para que esta a su vez presente a la línea estratégica.
			Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.
Tercera Línea de Defensa	Oficina de Control Interno	Realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la	**Asesorar** en coordinación con la Oficina Asesora de Planeación y la Dirección de Tecnologías, a la primera línea de defensa en el análisis y valoración del riesgo, y en el diseño de los controles.
			Verificar la publicación de los mapas de riesgos en el portal web institucional**.**
			Realizar seguimiento a la gestión de riesgos (analizar causas, riesgos, eficacia y efectividad de los controles), en los procesos que realice de auditorías internas.
		entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.	**Recomendar mejoras** a la política de administración del riesgo.
			Realizar evaluación a la gestión de Riesgos de la entidad.

Tabla 1. Esquema de Líneas de Defensa en la SDSCJ Fuente: Oficina Asesora de Planeación SDSCJ

El Comité Institucional de Gestión y Desempeño actúa como instancia superior para aprobación y seguimiento.

11 ANALISIS DE LOS OBJETIVOS ESTRATEGICOS Y DE LOS PROCESOS

Antes de iniciar la identificación de riesgos, es indispensable analizar los objetivos estratégicos de la entidad y su desdoblamiento en el objetivo del proceso. Estos objetivos deben ser coherentes con la misión y visión de la SDSCJ, y estar formulados bajo criterios SMART (específicos, medibles, alcanzables, relevantes y temporales).

Una formulación incorrecta de objetivos impide avanzar en la metodología de gestión del riesgo.

Se recomienda que cada proceso revise y, si es necesario, ajuste sus objetivos en la caracterización, para asegurar la identificación adecuada de riesgos que puedan afectar el cumplimiento del proceso y de los propósitos institucionales.

Un objetivo debe contar con las siguientes características:

Ilustración 2. Estructura de Un objetivo.
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas

Teniendo en cuenta la importancia del análisis de objetivos, a continuación se describe la importancia para cada tipología:

Riesgos de Gestión: Omitir este análisis puede llevar a identificar riesgos imprecisos, controles mal diseñados y pérdida de conexión con la planeación institucional, ya que a estos se definen como eventos que afectan el logro de dichos objetivos

Riesgos de Integridad Pública: Los riesgos de Integridad deben estar asociados a actividades críticas o vulnerables dentro de los procesos, y estas se derivan directamente del objetivo del proceso. Si no se tiene claridad sobre el objetivo del proceso, es difícil identificar los puntos críticos donde se pueden presentar riesgos como conflictos de interés, sobornos, fraude, lavado de activos o favorecimientos indebidos.

Riesgos Estratégicos: Por definición, los riesgos estratégicos afectan el cumplimiento de los objetivos estratégicos. Estos riesgos están directamente relacionados con los fines misionales de la entidad. Por ende NO se puede identificar un riesgo estratégico si no se ha hecho un análisis del objetivo estratégico que puede fracasar o verse afectado.

Riesgos Fiscales: Los riesgos fiscales están ligados al uso de los recursos públicos, cumplimiento de metas presupuestales y la ejecución financiera de los proyectos. Todos estos aspectos dependen del logro de objetivos institucionales y de proceso. Una deficiencia en la definición de objetivos (Ejemplo: metas de ejecución o cobertura) puede derivar en omisiones, ineficiencias o subejecuciones que pueden llegar a ser observaciones de entes de control.

12 IDENTIFICACIÓN Y GESTIÓN DE RIESGOS DE GESTIÓN

Partiendo de la “Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas” y una vez aclarados los anteriores lineamientos, es preciso contar con un diagnóstico del periodo finalizado, con el análisis del contexto enmarcado en el “Conocimiento de la Entidad” y la Gestión del “Modelo de Operación por Procesos” de esta forma, se establece el conocimiento y entendimiento de la Entidad, lo anterior, será determinante para el análisis de riesgos y la aplicación de la metodología en general, la cual se debe desarrollar por etapas, destacando la obligatoria participación del líder de proceso o líder operativo, quienes a su vez están a cargo de realizar una apropiada socialización con los funcionarios y contratistas que componen cada proceso.

Para cumplir satisfactoriamente con el objetivo de la correcta administración del riesgo, se hace necesario seguir las siguientes etapas detalladamente. Se enfatiza en el objetivo de identificar, analizar, dar tratamiento, seguimiento y evaluación a los

riesgos, logrando una visión integral de las actividades propias de la Entidad que podrían afectar el cumplimiento de las metas y objetivos trazados.

11.1. Conocimiento y Divulgación

La presente guia debe ser de conocimiento general para los funcionarios y contratistas de la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, se debe tener en cuenta que en este documento se especifican los lineamientos técnicos con los cuales se ejecuta la gestión del riesgo en la Entidad, por ende toda persona que interactúe con procesos y procedimientos debe actuar activamente en atención a la Gestión del Riesgo, considerando su conocimiento, punto de vista, percepciones y experiencia, propendiendo la mejor decisión evitando las posibles afectaciones y consecuencias por el desarrollo de actividades.

11.2. Apetito, Tolerancia y Capacidad del Riesgo

Para determinar el Apetito del Riesgo, Tolerancia del Riesgo y Capacidad del riesgo, es necesario revisar en primer lugar en Nivel del Riesgo para los Riesgos de Gestión los cuales detallamos a continuación, gráficamente:

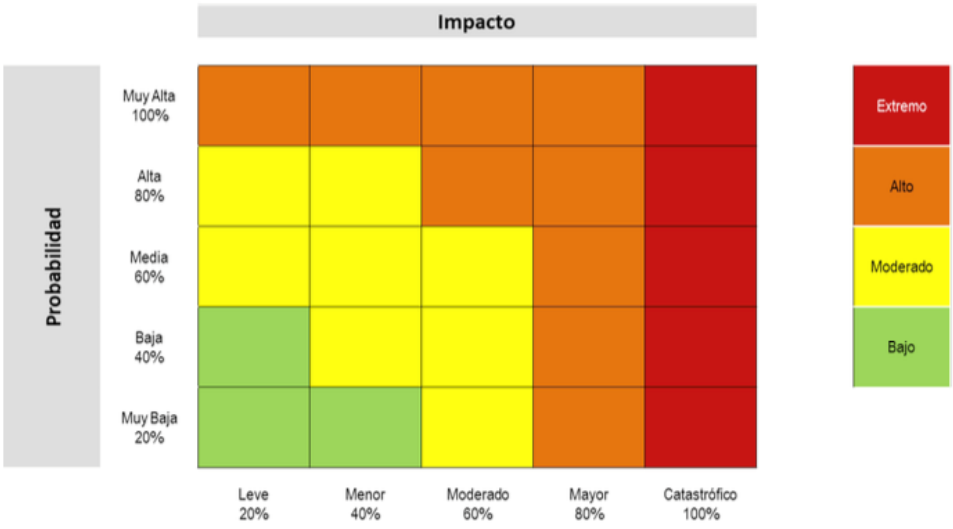

Ilustración 3. Matriz de Calor
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

Para ello, es necesario aclarar que el Nivel del Riesgo se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la

magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. Dado lo anterior, se establece lo siguiente:

Apetito del Riesgo: Nivel de Riesgo **Bajo**.
Tolerancia del Riesgo: Desde nivel de Riesgo Moderado - **Alto**.
Capacidad de Riesgo: Nivel de Riesgo **Extremo**.

Cabe aclarar que el Nivel de Riesgo Extremo es el valor máximo que, de acuerdo con lo establecido por la alta dirección, podrá ser resistido por la Entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Por ello todo lo que este por fuera del Nivel de Riesgo extremo deberá replantearse hasta tanto se definan nuevos valores de probabilidad e Impacto.

11.3. Identificación y análisis del Riesgo

Para poder establecer la identificación del Riesgo existen varios aspectos que combinados permitirán un correcto análisis de los procesos, se recomienda el uso de al menos uno de ellos, para ello se debe tener en cuenta:

- **Contexto externo:** Se examinan las características o aspectos esenciales del entorno en el cual opera la Entidad. Se pueden considerar factores como:
  - ✓ Políticos
  - ✓ Económicos y financieros
  - ✓ Sociales y culturales
  - ✓ Tecnológicos
  - ✓ Ambientales
  - ✓ Legales y reglamentarios
  - ✓ Grupos de interés externos y partes interesadas.
  - ✓ Clientes, proveedores de servicio y empresas.
  - ✓ Cantidad de ciudadanos afectados por la falta del servicio
  - ✓ Suplantación de identidad.
  - ✓ Asaltos/Vandalismo/Ataque terrorista/Orden Público a las instalaciones de la Entidad.

- **Contexto interno:** Se analizan cuáles son los rasgos distintivos que dictan la manera en la cual opera internamente la Entidad y busca alcanzar sus objetivos:
  - ✓ Misión
  - ✓ Visión
  - ✓ Valores
  - ✓ Estructura organizacional

- ✓ Funciones y responsabilidades
- ✓ Políticas, procesos y procedimientos. Objetivos y estrategias implementadas.
- ✓ Planes, programas y proyectos
- ✓ Sistema integrado de gestión.
- ✓ Recursos y conocimientos con que se cuenta (económicos, social, ambiental, físico, financiero, jurídico, Humano, procesos, sistemas, tecnología, información)
- ✓ Relaciones con las partes involucradas
- ✓ Cultura organizacional
- ✓ Infraestructura
- ✓ Servicios
- ✓ Tramites u otros procedimientos administrativos - OPA´S (Corrupción)

- **Contexto del Proceso:** Se revisan cuáles son las características o aspectos esenciales del proceso, si este está directamente relacionado con un objetivo estratégico de la Entidad, cuál es su alcance, cuáles son las entradas y las salidas derivadas de las actividades que se realizan en su interior:
  - ✓ Objetivo del proceso
  - ✓ Alcance del proceso
  - ✓ Caracterización del proceso
  - ✓ Interrelación con otros procesos
  - ✓ Procedimientos asociados
  - ✓ Responsables del proceso
  - ✓ Cantidad de ciudadanos afectados por el proceso
  - ✓ Procesos de gestión de riesgos actualmente implementados

11.4. Identificación y análisis de las actividades críticas del proceso

Dado que los objetivos estratégicos y el objetivo del proceso se alcanzan por medio de actividades, el paso a seguir corresponde a identificar las actividades cruciales para la consecución de los objetivos validando la integridad de la Caracterización del Proceso y los Procedimientos que lo componen, lo anterior es lo que se denomina Puntos de Riesgo dentro de la Cadena de Valor.

Ilustración 4, Cadena de valor
Fuente: Adaptado de la Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

11.5. Análisis por Eventos de Riesgo

Se puede indagar qué eventos de riesgo se podrían materializar que afectarían negativamente el alcance de los objetivos del proceso. Para ello podría plantear las siguientes preguntas:

- ✓ ¿Qué evento o Incidente negativo que afecte los objetivos del proceso puede suceder?
- ✓ ¿Cómo puede suceder este evento?
- ✓ ¿Cuándo podría suceder?
- ✓ ¿Qué consecuencias se podrían derivar de la materialización de este evento?
- ✓ Se redacta el evento de riesgo propendiendo, dar al lector y escucha una sensación que el riesgo ya se ha materializado.

Ilustración 5. Análisis de eventos
Fuente: Oficina Asesora de Planeación SDSCJ

A continuación, se presenta un ejemplo ficticio con la aplicación de estas preguntas:

- **¿Qué evento o Incidente negativo que afecte los objetivos del proceso puede suceder?** Liquidación inadecuada de un contrato.
- **¿Cómo puede suceder este evento?** Debido a una supervisión inadecuada del contrato que le dio el aval a los entregables por parte del contratista
- **¿Cuándo podría suceder?** Si se liquida el contrato sin cumplir con las especificaciones acordadas de los servicios o productos, o si se vencen los 4 meses siguientes a la expiración del término y las partes no han llegado a un acuerdo para finalizar a satisfacción el contrato generando consecuencias económicas y legales.
- **¿Qué consecuencias se podrían derivar de la materialización de este evento?** Pérdidas económicas, inicio de procesos jurídicos con afectación directa de la ejecución del procedimiento.

Es necesario aclarar que al definir el riesgo se debe evitar comenzar con palabras negativas como las siguientes palabras: “No”, “Que no”. O con palabras que denoten una causa como: “ausencia de…”, “falta de…”, “deficiente…”.

Algunas fuentes de eventos de Riesgos pueden ser:

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia
- Informes de auditoría Interna y Externa.

Es importante aclarar que los procesos de la Entidad deben incorporar a su gestión al menos un riesgo de gestión identificado, el cual debe estar debidamente estructurado en la Matriz Integrada de Riesgos, herramienta que ha sido definida por la Entidad para la administración del Riesgo.

11.6. Criterios Generales para decidir qué riesgos documentar

- ✓ Riesgos que puedan afectar el cumplimiento de los objetivos del proceso o de la entidad.
- ✓ Riesgos cuya materialización tenga impacto alto o extremo en dimensiones institucionales.
- ✓ Riesgos asociados a hallazgos, auditorías o planes de mejora vigentes.
- ✓ Riesgos que requieran controles significativos, seguimiento o tratamiento formal.
- ✓ Riesgos relacionados con corrupción, seguridad de la información, LA/FT o fiscales.

La definición final de los riesgos a documentar debe realizarse con participación del líder de proceso y del líder operativo – 1LD, con el acompañamiento metodológico de la Oficina Asesora de Planeación – 2LD. Estos riesgos deberán registrarse en la matriz oficial, publicada en el página web con el formato F-FI-1382.

11.7. Clasificación del Riesgo por Factor e Identificación de las causas

Para clasificar adecuadamente los riesgos se recomienda que se lleve a cabo un análisis de Matriz Contexto Estratégico - F-DE-1379 - esta es una técnica para organizar los factores internos y externos identificados en la etapa anterior y que afectan positiva o negativamente la forma en la cual una organización alcanza sus objetivos, o a través de herramientas de diagnóstico y/o análisis definidos por la Oficina Asesora de Planeación.

El ejercicio de la **DOFA** debe ser ejecutado adicionalmente en función de los objetivos estratégicos y los objetivos del proceso, y debe ajustarse las veces que sea necesario por cambios en las situaciones institucionales endógenas o exógenas.

Ilustración 6. DOFA
Fuente: Oficina Asesora de Planeación SDSCJ

Las **debilidades** y **fortalezas** son de carácter interno y provienen del análisis del contexto o factor internos del proceso. De otro lado, las **oportunidades** y las **amenazas** corresponden al análisis del contexto o factor externo de la Entidad y del proceso.

Ilustración 7 Contextos Asociados
Fuente: Oficina Asesora de Planeación SDSCJ

De manera complementaria, se establece un listado con los factores de riesgo que pueden incidir en el proceso, los cuales podrán ampliarse o adecuarse de acuerdo con las características propias de cada proceso o cambios en las situaciones institucionales, y que deban ser contemplados para una adecuada identificación del riesgo, y que desarrolla los riesgos para la integridad pública.

Clasificación	Descripción
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.

Tabla 1. Clasificación
Fuente: Oficina Asesora de Planeación SDSCJ

Una vez este diligenciada la matriz DOFA, si se observan las casillas de **Debilidades** y **Amenazas**, en ellas están consignadas las causas más significativas que facilitan la materialización de los eventos de riesgo.

Las siguientes son las fuentes generadoras de Riesgo:

Factor	Definición	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servideres de la organización. Estructura organizacional que afecta la capacidad organizacional.	Falta de aplicación de los procedimientos Falta segregación de funciones Errores de grabación, autorización Falta de supervisión o interventoría Errores en cálculos para pagos internos y externos. Alta rotación o insuficiencia de personal Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en et trabajo
Talento Humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la integridad Pública.	Fraude interno Soborno Gestión inadecuada de conflicto de intereses
Tecnologia	Eventos relacionados con la infraestructura tecnologica de la entidad.	Errores en cálculos para pagos internos y externos Alta rotación o insuficiencia de personal Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en et trabajo
Tecnologia	Eventos relacionados con la infraestructura tecnologica de la entidad.	Daño de equipos Caida de sistemas de información y aplicaciones Errores en hardware o software
Infraestructura	Eventos relacionados con la infraestructura fisica de la entidad.	Derrumbes Caida de sistemas de información y aplicaciones Caida de redes
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transaccciones o operationes realizades por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a traves de los conlies	Errores en hardware o software Errores en programas Daños a activos fijos
Evento Externo	Eventos por situaciones externas que afectan la entidad.	Fraude externo Suplantación de identidad Asalto a la oficina Atentados, vandalismo, orden público

Ilustración 8 Factores de Riesgo
Fuente: Oficina Asesora de Planeación SDSCJ

Identificado lo anterior, se debe establecer la Causa Inmediata y la Causa Raíz de acuerdo con lo siguiente:

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 analizarse.
El análisis de causas lo puede desarrollar utilizando la siguiente metodología de priorización:

- ✓ Listar causas a partir del riesgo identificado.
- ✓ Cada integrante priorizará en orden de importancia de menor a mayor las causas utilizando una escala donde 1 es la de menor importancia y «N» la de mayor importancia dependiendo del número de causas.
- ✓ Un integrante del grupo debe organizar en la tabla las calificaciones y calcular el promedio aritmético de cada causa, siendo las de mayor promedio **las causas raíz.**

No	Causa (amenazas y debilidades)	Observador 1	Observador 2	Promedio
1	Causa 1	…	…	
2	Causa 2	…	…	
N	Causa N	…	…	

Tabla 2. Tabla de priorización
Fuente DAFP

11.8. Estructura de Redacción

El impacto está definido como la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Por ello, los impactos que se aplican a la Secretaría Distrital de Seguridad, Convivencia y Justicia, son **afectación económica y reputacional**.

Dado lo anterior, la siguiente será la estructura del Riesgo:

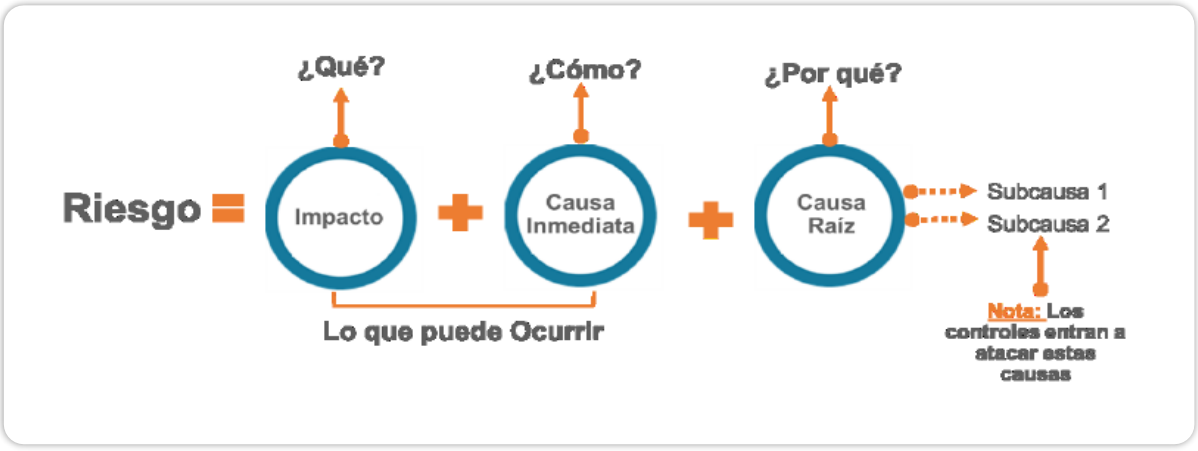

Ilustración 9. Estructura de Redacción Riesgos de Gestión
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

La descripción del riesgo debe contener todos los detalles antes ilustrados con la intención de que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. La estructura facilita su redacción y claridad, 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.

La redacción siempre debe iniciar con la frase " ***Posibilidad de*** ", a continuación un ejemplo:

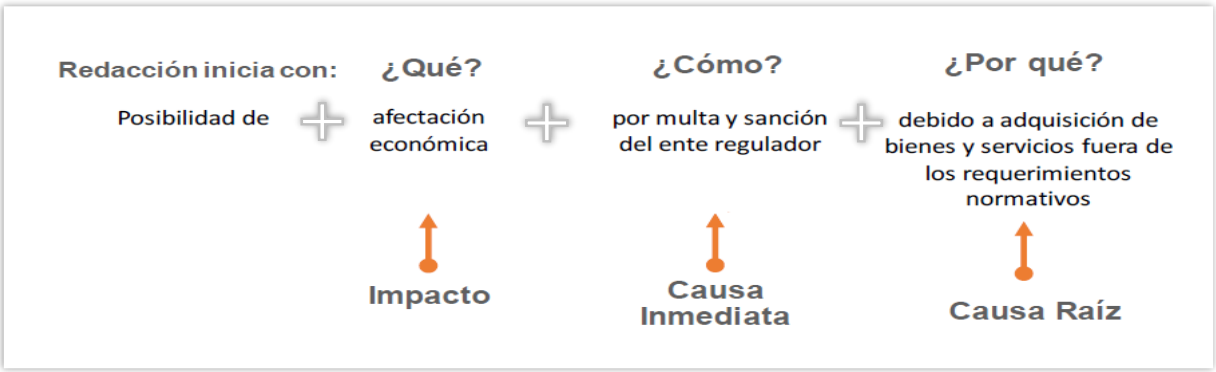

Ilustración 10. Ejemplo de redacción Riesgo de Gestión
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

Tener en cuenta al redactar el 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.

11.9. Valoración del riesgo

En esta etapa se busca determinar la probabilidad de ocurrencia del riesgo junto con el impacto o consecuencias que traería. La probabilidad de ocurrencia está 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.

Para determinar la probabilidad se toma como referencia la siguiente tabla de probabilidades valorada por niveles acorde a los lineamientos del DAFP:

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%

Tabla 3. Calificación de Probabilidad
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

De igual forma para determinar el impacto económico y reputacional se cuenta con la siguiente tabla que es valorada por niveles de la siguiente forma:

Niveles de Impacto	Afectación Económica	Afectación Reputacional	Impacto

Leve	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	20%
Menor	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.	40%
Moderado	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la Entidad con algunos usuarios de relevancia frente al logro de los objetivos.	60%
Mayor	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.	80%
Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la Entidad a nivel nacional, con efecto publicitario sostenido a nivel país	100%

Tabla 4. Calificación de Impacto
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

Una vez determinada la probabilidad (P) y el impacto (I) del riesgo, la combinación de estas nos ofrece el nivel de riesgo inherente *(**riesgo inherente**: es el nivel de riesgo sin que aún se le haya aplicado ninguna media para mitigarlo),* se obtiene ubicando la posición de acuerdo con la valoración obtenida de cada variable en la siguiente matriz de calor.

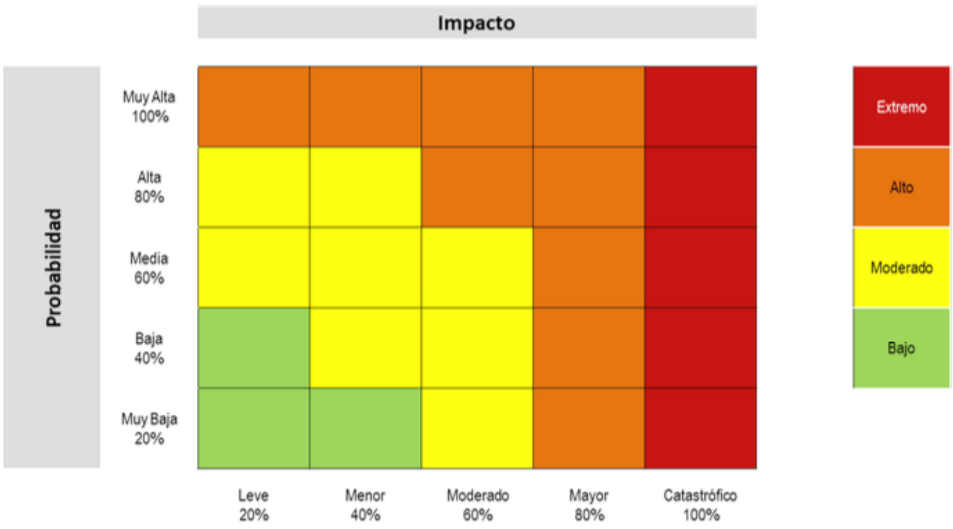

Ilustración 11. Matriz de Calor
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

La matriz de calor cuenta con cinco niveles de ubicación para la probabilidad y cinco niveles para el impacto, los cuales combinados ofrecen cuatro zonas determinadas por zonas y colores Bajo, Moderado, Alto y Extremo

12.1 Creación de Controles

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.

12.2 Estructura de Controles

Para definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

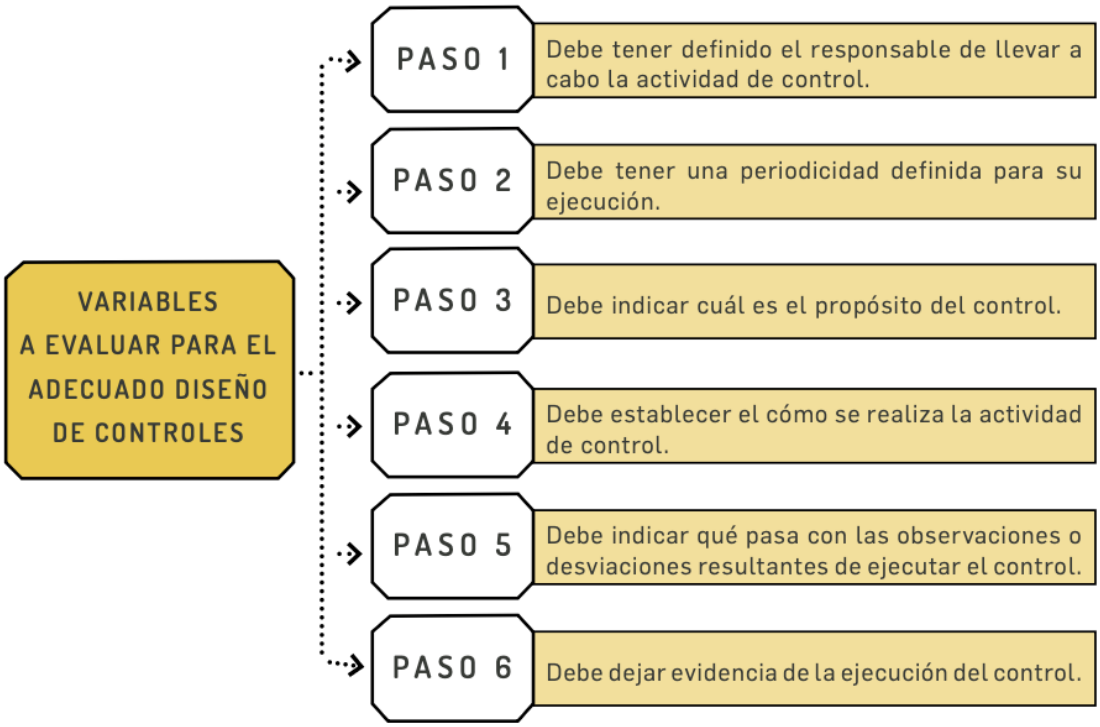

Ilustración 12. Pasos para diseñar un control
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

- El **responsable de su ejecución** debe identificar claramente el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identifica el sistema que realiza la actividad. (Evitar asignarlo a áreas generales o nombres propios), por ejemplo: responsable de inventarios.

- El propósito del control es la descripción del control se debe especificar como se ejecuta **la Acción** del control recuerde que las acciones podrían ser **verificar**, **validar, cotejar, comparar** "algo respecto algo"…

Detalles adicionales que permiten identificar claramente la ejecución del control:

- La ejecución del control **debe tener un soporte documental**, por ejemplo, una base de datos, una lista de chequeo, un acta de reunión, etc.
- En la definición del control se debe especificar cuál es la **periodicidad de la aplicación** de este; por ejemplo: *el coordinador debe revisar (mensualmente, trimestralmente, cada vez que se presente…)*
- La definición del control debe incluir en que situaciones se presentan **desviaciones entre el resultado esperado y el resultado obtenido** y que **acciones se deben tomar si se presentan dichas desviaciones.**

La siguiente es la estructura para los controles recomendada.

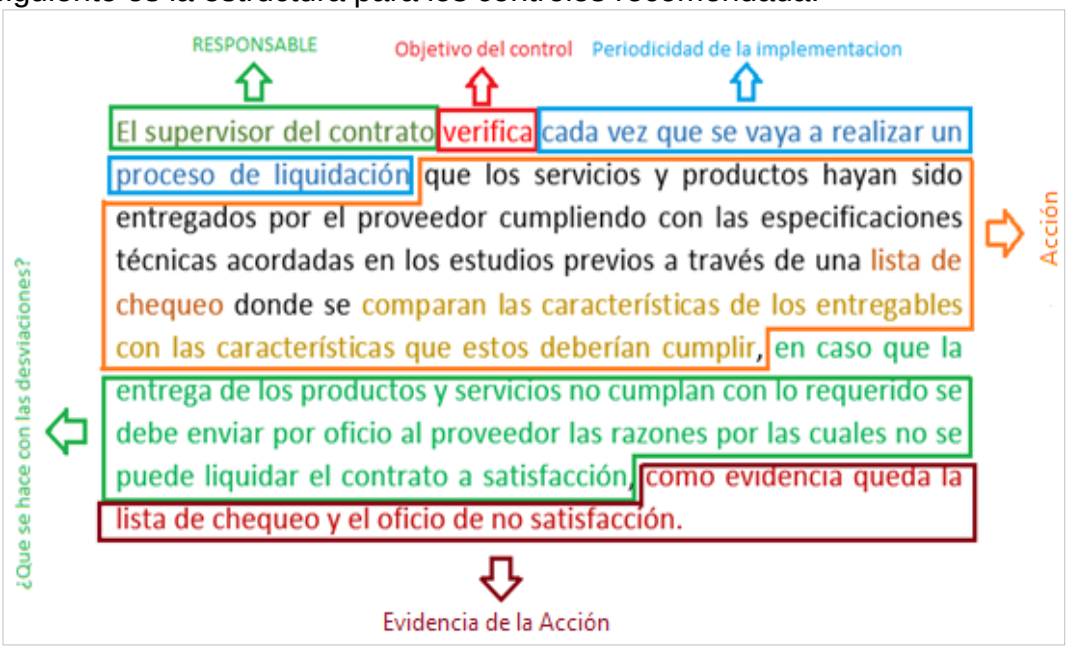

Ilustración 13, Ejemplo de redacción de un control
Fuente: Oficina Asesora de Planeación SDSCJ

Notas:

- *Para aquellos casos en los cuales la actividad control represente el manejo de **información reservada o clasificada** deberá mencionarse dentro de la actividad control y se deberá aclarar dentro del mismo que tipo de evidencia se recibirá.*
- *En caso de no haber ejecutado el control durante el periodo se deberá suministrar la justificación que indique el motivo por el cual el Control no se ejecutó.*
- *La manera en la cual se lleva a cabo su ejecución debe estar documentada en alguno de los documentos del MIPG (por ejemplo, en un procedimiento, un manual, un instructivo, etc.), sin querer decir que la existencia de dicho documento donde esta consignada esta información sirva como el control per se.*

- *La causa Raíz del riesgo se debe atender con **por lo menos un control** asignado a su mitigación.*

12.3 Tipos de controles

Se tienen tres tipos de controles en función al ciclo del proceso en el cual se ejecutan (**Eficiencia)**:

Control Preventivo: (Entrada) Buscan evitar que el evento de riesgo se materialice (disminuyen la probabilidad) y están orientados a atacar las causas que facilitan la materialización del evento de riesgo. 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: (Interrelaciones) Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad de ocurrencia del riesgo. Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
Controles Correctivos: (Salida) Atacan el impacto frente a la materialización del riesgo. Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

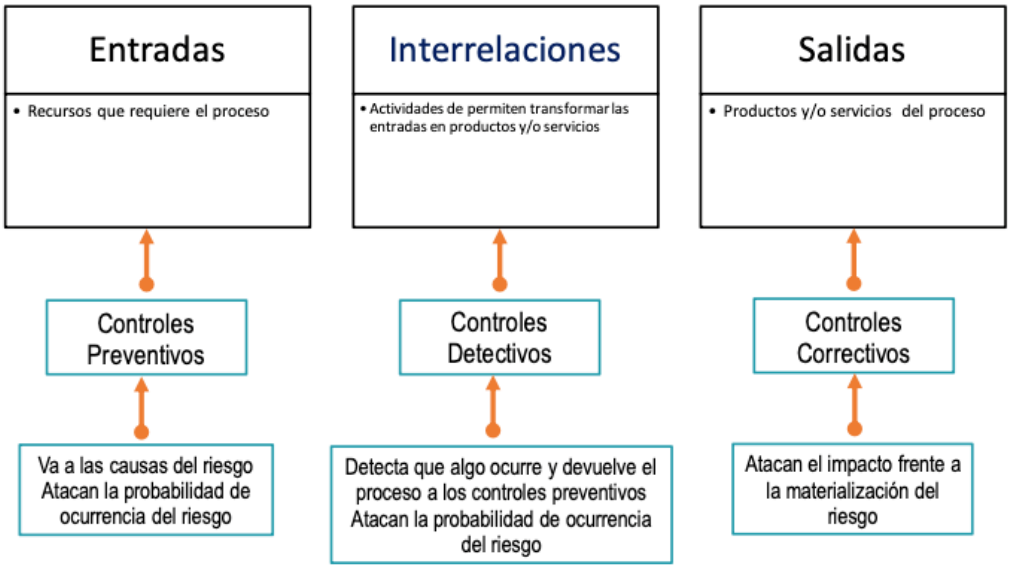

Ilustración 14. Tipologías de Controles y su efecto sobre probabilidad e impacto
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

De acuerdo a la forma en que se ejecutan, se tienen las siguientes:

Control Manual: controles que son ejecutados por personas.
Control Automático: son ejecutados por un sistema.

12.4 Calificación del control

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia e implementación.

Esta evaluación está a cargo del profesional de la gestión del riesgo de la Oficina Asesora de Planeación de la SDSCJ en acompañamiento del líder operativo del proceso, en algunos casos se podrá contar con la participación de los servidores que ejecuten las actividades.

En cumplimiento de las características mencionadas en el ***numeral 11.7.2 "Tipos de Controles"***, cada una tiene un peso específico y no pueden existir respuestas diferentes a las relacionadas:

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%
Atributos informativos de cumplimiento		**Responsable**	Cuenta con responsable del Control	-
		Documentado	Documentado / Sin Documentar	-
		Evidencia	Se tiene Evidencia de la ejecución del control	-
		Desviaciones	Se tienen en cuenta las deviaciones	-
		Periodicidad de ejecución	Se ejecuta con una periodicidad adecuada	-

Tabla 5. Peso Diseño del Control
Fuente: Oficina Asesora de Planeación SDSCJ

Los atributos informativos dan formalidad al control (no tienen peso), no obstante, se requieren para conocer el entorno del control y complementar el análisis con elementos cualitativos mas no tienen incidencia directa en su efectividad1.

12.5 Evaluación de Ejecución del Control

No solo basta con que el control esté debidamente diseñado, sino también se tiene que velar por su implementación y ejecución cumpliendo con las responsabilidades de cada línea de defensa, para lo cual, se define la calificación de la ejecución del control con base en la siguiente tabla:

Rango de Calificación de la Ejecución	Resultado - Peso de la Ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Tabla 6. Evaluación Ejecución del Control
Fuente: Oficina Asesora de Planeación SDSCJ

La Oficina Asesora de Planeación realizara el acompañamiento y asesoría a los procesos para el diseño y reporte de los controles, realizará el seguimiento y emitirá conceptos técnicos de mejora. Por su parte, la Oficina de Control Interno será la encargada de realizar la evaluación y asesoría en las mejoras del caso, a los procesos que lo ameriten.

12.6 Validación de evidencias del Control

La Oficina Asesora de Planeación, dentro de sus funciones de segunda línea de defensa, es la responsable de:

1 ***Los riesgos no se pueden cubrir al 100% (Por ello la calificación máxima de un control es 50%), el control cubre una parte pero siempre se va a tener un riesgo residual aunque se implementen muchos controles.***

- verificar la consistencia metodológica de la gestión del riesgo
- validar las evidencias reportadas por los procesos
- emitir observaciones y recomendaciones
- consolidar los resultados de la validación
- elaborar los informes de seguimiento institucional a riesgos.

La validación realizada por la OAP se rige por los siguientes principios:

Independencia técnica: La validación no sustituye la responsabilidad de la primera línea.
Trazabilidad: Toda evidencia debe permitir identificar el control ejecutado, la fecha y el responsable.
Pertinencia: La evidencia debe corresponder al control definido en la matriz de riesgos.
Oportunidad: Las evidencias deben cargarse dentro de los tiempos establecidos para cada tipo de riesgo.
Consistencia metodológica: La información debe ser coherente con la valoración del riesgo y el diseño del control.

Se consideran evidencias válidas para la validación de controles: informes técnicos, actas de reunión, registros en sistemas de información, reportes de monitoreo, capturas de sistemas institucionales, bases de datos, documentos administrativos, reportes de indicadores, registros de auditoría, comunicaciones oficiales; en todo sentido, las evidencias deben permitir verificar la ejecución objetiva del control.

12.7 Criterios de validación de evidencias

La Oficina Asesora de Planeación verificará los siguientes criterios:

Criterio	Descripción
Existencia	La evidencia fue cargada en el repositorio
Correspondencia	La evidencia corresponde al control definido
Integridad	La evidencia está completa
Oportunidad	Fue cargada dentro del plazo establecido
Pertinencia	Permite demostrar la ejecución del control
Trazabilidad	Permite identificar responsable y fecha

Por su parte la Oficina de Control Interno será responsable de:

- evaluar de forma independiente la gestión del riesgo

- verificar la efectividad del sistema de control interno
- emitir recomendaciones de mejora.

12.8 Nivel de Riesgo Residual

A partir de los controles estructurados y el peso obtenido por los mismos de acuerdo con lo establecido en el anterior numeral se obtiene el movimiento en la matriz de calor, lo que da como resultado nuestro Riesgo Residual que corresponde al movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

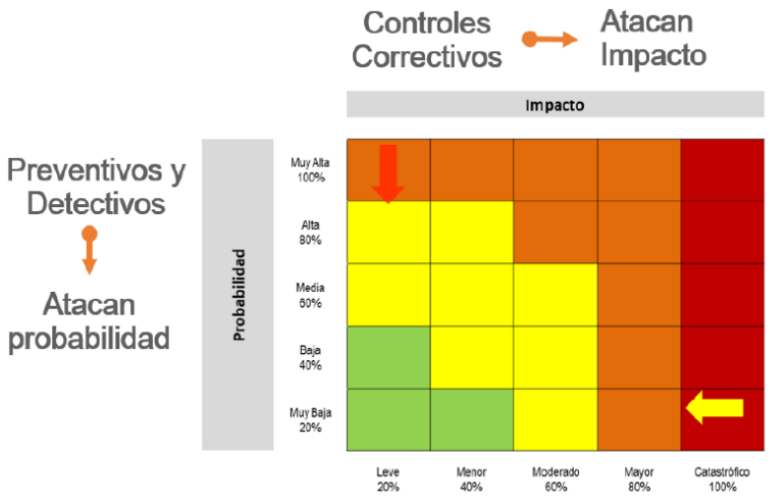

Ilustración 15. Movimiento en la matriz acorde al tipo de control
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplica con el valor resultante luego de la aplicación del primer control. A su vez se procede por separado tanto para Probabilidad como para impacto.

PROBABILIDAD

La formulación es la siguiente:

Probabilidad Inherente = PI
Valoración Control Preventivo = VCP
Probabilidad Residual$_1$ = PR$_1$

$$PR_1 = PI - (PI * VCP)$$

Para las situaciones en las cuales se cuente con controles Detectivos se procederá continuara con la aplicación de la Formula:

Probabilidad Residual$_1$ = PR$_1$
Valoración Control Detectivo= VCD
Probabilidad Residual$_n$ = PR$_n$

$$PR_n = PI_1 - (PI_1 * VCD)$$

Para los casos en los cuales se cuente con más controles se continuará ejecutando la formula hasta agotar la cantidad de Controles estructurados siempre otorgando prioridad a las tipologías con el siguiente Orden: Preventivo-Detectivo

IMPACTO

La formulación es la siguiente:

Impacto Inherente$_1$ = II$_1$
Valoración Control Correctivo= VCC
Impacto Residual$_n$ = IR$_n$

$$IR_n = II_1 - (II_1 * VCC)$$

Con lo anterior, se determina la posición del riesgo después de la ejecución del control(es) considerando que están correctamente diseñados y que en efecto estos mitigan las causas, evitando que el riesgo se materialice. De solo contar con Controles Preventivos y Detectivos solo se lograra la disminucion de la Probabilidad. Si solo se cuenta con controles Correctivos solo se lograra disminucion de Impacto. ***La Diferencia entre el Nivel de Riesgo Inherente y el Residual es lo que se denomina Eficiencia del control.***

Por lo anterior y para garantizar que el control elaborado se está efectuando, se hace necesario el seguimiento a la ejecución de éste. La Oficina Asesora de Planeación ha puesto a disposición una carpeta compartida en SharePoint, que ha sido socializada con los líderes operativos y de proceso en la cual se deberán ubicar las evidencias que permitan avalar y corroborar la ejecución respectiva por la Segunda y Tercera Línea de Defensa.

Los periodos de corte para la entrega de evidencias y posterior elaboración de informe son indicados en Política de Administración de Riesgos.

12.9 Tratamiento del Riesgo Residual

Dada la Zona de Riesgo Residual obtenida con la ejecución de controles, se realiza un tratamiento a los riesgos identificados2 que se aplica de la siguiente forma:

Aceptar el riesgo3: valido únicamente para aquellos cuya zona de riesgo residual **es baja** no se aplica ninguna acción adicional a la ejecución permanente del control que se tiene estipulado asumiendo el mismo conociendo los efectos de su posible materialización.

Reducir el riesgo: para aquellos cuya Zona de Riesgo Residual sea **diferente a baja**, se deberán toman acciones mediante Transferencia o Mitigación previa realización de un análisis de la situación dejando evidencia en la Matriz de Riesgos:

- ✓ **Mitigar:** esto se logra por medio de acciones que mitiguen el nivel de Riesgo, no necesariamente se refiere a la implementación de controles adicionales.
- ✓ **Transferir:** estrategia de tercerización del proceso o traslado del riesgo a través de seguros o pólizas. La responsabilidad económica recaerá sobre el tercero. Sin embargo, se mantiene la responsabilidad reputacional.

Para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo. Toda vez que **ningún riesgo de corrupción podrá ser aceptado.**

13 IDENTIFICACIÓN Y GESTIÓN DE RIESGOS DE INTEGRIDAD PÚBLICA

13.1 Definición y alcance

“El SIGRIP busca articular la Política para la Gestión Integral de Riesgos mediante la cual se gestionan los Riesgos Generales de la Gestión, la Gestión Preventiva de Riesgos Fiscales y los Riesgos de Seguridad de la Información, con los demás elementos que son necesarios para gestionar los riesgos para la integridad pública,

2 ***Nota 1: El líder del proceso puede tomar la decisión de aceptar el riesgo y no será necesaria la implementación de una medida de mitigación***.

3 ***Nota 2: No Aplica para Riesgos de Integridad***

que se describen a continuación.

Al final, un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causa el soborno, el fraude, un conflicto de intereses gestionado inadecuadamente o la corrupción. Además, puede también favorecer el lavado de activos, la financiación del terrorismo o la financiación de la proliferación de armas de destrucción masiva.

Por esta razón, es necesario abordar los riesgos para la integridad pública de forma integral y en estrecha articulación con la gestión institucional del riesgo. La valoración del riesgo de integridad consiste en el análisis y evaluación de las situaciones en las que la acción u omisión de un servidor público o contratista puede afectar los intereses de la Secretaría Distrital de Seguridad, Convivencia y Justicia, desviándose de los valores éticos, los deberes legales y el compromiso con el servicio al ciudadano.

En este mismo sentido, se deben diseñar herramientas instruccionales de administración de riesgos que permita proteger a la SDSCJ ante el posible riesgo asociado al lavado de activos (LA) y Financiación del Terrorismo (FT) y dar cumplimiento a las obligaciones que se establecen en la normatividad vigente. De este modo, la SDSCJ se acoge a la recomendación de asociar y articular a la gestión de riesgos de integridad pública, los eventos que se identifiquen analicen y evalúen de riesgos asociados a LA/ FT, fraude, soborno, conflicto de interés y corrupción.

13.2 Conocimiento y divulgación

Los riesgos se deben dar a conocer a todo el equipo del proceso; la Oficina Asesora de Planeación realizará la divulgación del informe de riesgos al Comité Institucional de Gestión y Desempeño.

La siguiente información se puede detallar, verificar y validar en la Matriz Integrada de Riesgos de la SDSCJ, la cual debe ser publicada y dada a conocer, a través de la Intranet y en la página WEB de la SDSCJ en los espacios definidos para tal fin.

13.3 Identificación y análisis de las causas

El ejercicio se realiza partiendo de los eventos identificados y se procede con el análisis de los siguientes aspectos de forma individual:

- Proceso(s) responsables.
- Amenazas y Debilidades asociadas de acuerdo con la Matriz DOFA de la Entidad la cual debe actualizarse periódicamente de acuerdo con la realidad operativa del proceso.
- Formulación mediante el Metalenguaje de causas, riesgo y consecuencias (debido a – Podría suceder – lo que generaría) teniendo en cuenta que las Amenazas y Debilidades se pueden tomar como causas.

Entre las causas analizadas se contemplan las siguientes situaciones:

- ✓ Procesos que involucran trámites que implican manejo de dinero en efectivo.
- ✓ Falta de segregación de funciones por restricciones de planta.
- ✓ Arqueos de caja adelantados por personal no idóneo y sin la autoridad requerida (adelantada por el mismo servidor o bien por otro servidor que no cuenta con un nivel jerárquico superior).
- ✓ Gestión Documental con fondos acumulados que no garantizan los registros y memoria institucional.
- ✓ Fases de análisis de los requisitos con excesiva reserva que impida la transparencia en determinado proceso.
- ✓ Falta de herramientas tecnológicas para la transmisión de datos e información entre procesos y a nivel externo.
- ✓ Inexistencia de archivos contables.
- ✓ Discrecionalidad para la toma de decisiones en grupos restringidos de servidores.
- ✓ Ausencia o debilidad de medidas y/o políticas para la identificación y manejo de conflictos de interés.

Para identificar estos riesgos en los procesos de la Secretaría, se deben considerar los siguientes factores, adicionales a los definidos en la ilustración No 8 “Factores de Riesgo”, así mismo en lo incluido en la matriz integral de riesgo:

- ✓ Conflicto de intereses: Situaciones donde el interés personal interfiere con el deber público.
- ✓ Abuso de funciones: Uso de la autoridad para fines distintos a los misionales.

- ✓ Tráfico de influencias: Utilizar la posición para beneficiar a terceros en trámites o contratos.
- ✓ Uso indebido de información privilegiada: Especialmente sensible en el manejo de datos de seguridad y convivencia ciudadana.

13.4 Estructuración del riesgo de integridad[4]

Con el fin de facilitar la identificación de riesgos de integridad y evitar que se presenten confusiones entre un riesgo de gestión u otra clase, se debe utilizar la matriz integral de riesgos, donde establecen los factores de riesgo.

Para los casos en los cuales no se cumpla con la información requerida, se deberá reevaluar el riesgo, dado que por definición no haría parte de los Riesgos de Integridad sino a un Riesgo de Gestión.

13.5 Análisis del Riesgo (Impacto y Probabilidad).

En esta etapa se busca determinar cuál es el nivel de riesgo derivado de la probabilidad de materialización del riesgo junto con el impacto que este tendría en los objetivos del proceso. La manera en la cual se establece la probabilidad para un riesgo de corrupción está dada los siguientes criterios:

Se debe evaluar la frecuencia con la que se presentan las vulnerabilidades:

- ✓ **Rara vez:** No existen antecedentes y los controles preventivos son sólidos.
- ✓ **Improbable:** Existen pocos incentivos para la falta de integridad.
- ✓ **Posible:** El proceso tiene contacto directo con el público o manejo de recursos.
- ✓ **Probable:** Se han detectado debilidades en la cultura organizacional del área.
- ✓ **Casi seguro:** Antecedentes de quejas o investigaciones recurrentes.

De manera articulada, los Riesgos de Integridad hacen uso de tres niveles de impacto (moderado, mayor y catastrófico), proyectando la posibilidad de materialización del riesgo afectando o generando alguna de las situaciones descritas en la matriz.

A título informativo se presentan los rangos de análisis y evaluación para los Riesgos de Integridad, condensados en la matriz integral de riesgos:

---

4 **Nota: Es importante tener en cuenta que un riesgo de integridad usualmente se caracteriza por la existencia de dolo, de la intención de obtener un beneficio indebido (propio o de un tercero) aprovechándose de la posición, trasgredir las normatividad y leyes.**

PROBABILIDAD				
Nivel	**Frecuencia de la Actividad**	**Mínimo**	**Máximo**	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	0	2	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	3	24	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	25	500	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5.000 veces por año	5001	5000	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año	5001		100%

Tabla 7Probabilidad

IMPACTO			
Nivel	**% Impacto**	**Afectación_Económica**	**Reputacional**
Leve	20%	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

Tabla 8 Impacto

A continuación, representamos el mapa de calor en cual se ubica el riesgo inherente para un evento asociado a integridad pública, luego de su identificación:

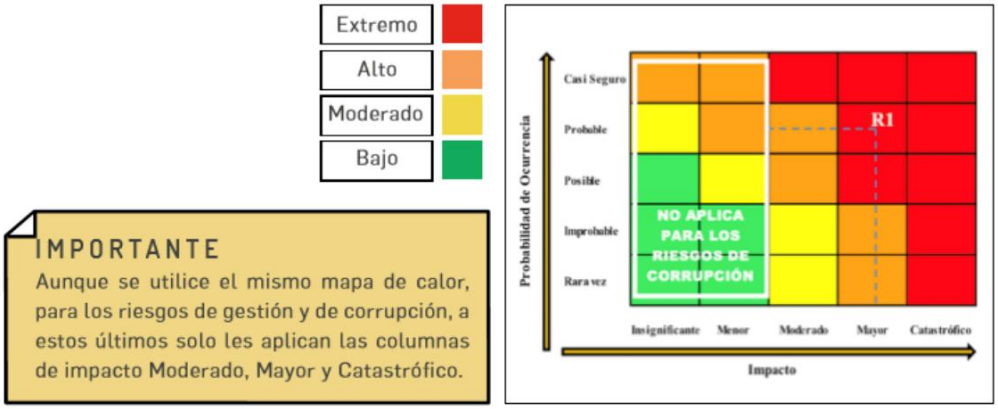

Ilustración 16. Matriz de Calor de Corrupción
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

En el caso de los Riesgos de Integridad se destaca que no se puede aceptar ningún riesgo sin haberse aplicado algún tratamiento. Las medidas son: **Reducir el riesgo** (implementar un control), **Evitar el riesgo** (dejar de realizar la actividad con la cual está relacionada el riesgo) o **Compartir el riesgo** (transfiriéndolo o compartiéndolo con un agente externo al proceso implementando un nuevo control).

Adicionalmente, se debe especificar que el nivel de Riesgo Residual (el nivel de riesgo que resultante después de aplicar las medidas de mitigación que se han adoptado), no siempre va a cambiar luego de la aplicación de los controles, lo anterior dado que el impacto no tendrá modificaciones por tratarse de Riesgos de Integridad, de esta manera es necesario garantizar el seguimiento y calidad de las evidencias a la ejecución de los controles y que estos sean suficientes para garantizar que el riesgo no se materialice.

13.6 Tratamiento del riesgo de integridad.

Teniendo en cuenta que los niveles de impacto establecidos para los riesgos de integridad son **Moderado, Mayor** y **Catastrófico** no se admite que ninguna línea de defensa tome la decisión de no aplicar una medida de reducción al riesgo inherente.

Se destaca que las medidas son:

- **Reducir el riesgo:** Se toman acciones para disminuir la probabilidad y/o el impacto, esto se logra por medio de la implementación de controles.
- **Evitar el riesgo:** Se elimina la implementación de las actividades críticas que facilitan la materialización del riesgo.
- **Compartir el riesgo:** Se busca disminuir el impacto y/o la probabilidad del riesgo compartiéndolo con otro proceso de la Entidad o con un actor tercero, por ejemplo, mediante una póliza de seguro con una compañía exógena a la Entidad.

Si el líder del proceso decide que la acción de tratamiento al evento de riesgo será la de **reducir el riesgo** o **compartir el riesgo** se debe representar mediante una actividad de control, la cual podrá ser diseñada por el líder operativo en compañía del apoyo metodológico del Profesional de Riesgos designado por la Oficina Asesora de Planeación.

13.7 Creación de Controles

Para la creación de controles, se mantiene la metodología general (remítase al apartado **Creación de controles)**, no obstante, se tienen dos tipos de controles aplicables a esta tipología de Riesgos:

Control preventivo: buscan evitar que el evento de riesgo se materialice (disminuyen la probabilidad) y están orientados a atacar las causas que facilitan la materialización del evento de riesgo. (ejemplo: Código de Integridad, capacitaciones en ética pública, declaraciones de bienes y rentas)

Control detectivo: buscan identificar la situación no deseada, una vez se haya presentado, y tiene por objetivo minimizar el impacto de la materialización del evento de riesgo, por eso este tipo de riesgo está encaminado a disminuir las consecuencias del riesgo. (ejemplo: Línea 195, buzones, auditorías de cumplimiento y seguimiento a procesos de contratación.)

13.8 Nivel de riesgo residual

Tras aplicar los controles, se obtiene el Riesgo Residual. Si el nivel de riesgo aún es "Alto" o "Extremo", se deben definir acciones de tratamiento inmediatas en el Plan de Acción Institucional.

Dada la Zona de Riesgo Residual obtenida con la ejecución de controles, se realiza un tratamiento a los riesgos identificados que se aplica de la siguiente forma:

- **Reducir el riesgo:** Se deberán toman acciones adicionales para disminuir la probabilidad y/o el impacto, esto se logra por medio de la implementación de controles adicionales que deberán analizarse dentro de un periodo de tiempo, cuyo limite es la finalización del Año que se encuentre en curso y dependiendo del resultado deberán incluirse como Controles para el siguiente Año.
- **Evitar el riesgo:** Se elimina la ejecución de las actividades que facilitan la materialización del riesgo.
- **Compartir el riesgo:** Se busca disminuir el impacto y/o la probabilidad del riesgo compartiéndolo con otro proceso de la Entidad o con un actor tercero, por ejemplo, mediante una póliza de seguro con una compañía exógena a la Entidad que deberán ser analizados dentro de un periodo de tiempo, cuyo limite es la finalización del año que se encuentre en curso y dependiendo del resultado deberán ser incluidos como Controles para el siguiente año.

14 IDENTIFICACIÓN Y GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

En la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, la gestión del riesgo en seguridad de la información, hace parte de esta Política de Administración de Riesgos, en la cual se identifican: tipo de amenazas, vulnerabilidades, Impacto, niveles de riesgos, y tratamientos con base en los activos de información alineado a las Tablas de Retención Documental, cumpliendo con los lineamientos para la gestión de riesgos en Seguridad digital en las Entidades públicas de acuerdo a la establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI), del Ministerio de Tecnologías de la Información – MINTIC, metodología definida. Aplicar formato Matriz de Riesgos de Seguridad de la Información F-FI-1385, así:

14.1 Conocimiento y Divulgación

Esta política debe ser de conocimiento general para los funcionarios directos e indirectos vinculados a la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, en el cual se especifican los lineamientos técnicos a seguir en la ejecución de la gestión del riesgo en la Entidad, con el fin de asegurar la integridad, disponibilidad, y confidencialidad de la información de sus procesos.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información esta publicado en la página web e intranet, en las siguientes rutas:

Intranet. Lineamientos y normatividad - Transparencia (planes - matriz de riesgo) - políticas, lineamientos y manuales - Plan estratégicos sectoriales e instituciones - Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

WEB. https://scj.gov.co/es Transparencia y Acceso a la información pública – Planeación, presupuestos e informes – Plan de Acción - Plan estratégicos sectoriales e instituciones- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

14.2 Identificación de los activos de seguridad de la información

Para la identificación de riesgos de seguridad de la información es preciso identificar los activos de información de los procesos de gestión de la Secretaría Distrital de Seguridad convivencia y Justicia acorde a la G-GD-01 Guía De Gestión De Activos De Información E Índice De Información Clasificada Y Reservada, los cuales deben ser clasificados y valorados teniendo en cuenta que en el contexto de seguridad de la información, estos se refieren a: Información, Hardware, software, Servicio, Recurso Humano, Otros que se utilizan para el funcionamiento.

La identificación y valoración de activos de información será realizada por la **Primera Línea de Defensa** – **líderes de proceso**, en donde se identifiquen riesgos de seguridad de la información, orientados por el profesional **responsable de seguridad de la Información** y personal de la Dirección de **Recursos Físicos y Gestión Documental**, de acuerdo con los siguientes pasos, así:

14.3 Pasos para la identificación y/o valoración de activos

La identificación de los activos de información en la Entidad se realiza de forma conjunta entre: los profesionales de Seguridad de la Información, Recursos Físicos y Gestión Documental y los líderes de los procesos teniendo en cuenta lo siguiente:

Ilustración 17, Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC

a. Información del Proceso

Registrar la información del proceso de acuerdo con lo definido en la Guía de Gestión de Activos de Información y el formato Registro de Activos de Información:

- **ID:** Numero consecutivo de Identificación - **(AI0001).**
- **Tipo De Proceso:** Seleccione de la lista el tipo de proceso (Estratégico, Misional, Apoyo, Seguimiento y Control) al que se le identificará los activos de información.
- **Proceso:** Identificar el proceso al que pertenece el activo. (**21 procesos**)
- **Código Del Procedimiento:** relacionar el procedimiento que corresponda al activo de información que se establece.
- **Código Del Formato:** Registrar el código asignado al formato dentro del SIG, del cual se genera el documento de archivo o registro.

b. Tipo Documental.

Se establece información del activo, de acuerdo con lo establecido en la Guía de Gestión de Activos de Información de la Entidad.

- **Nombre Del Activo:** Asignar el nombre correspondiente a cada activo de información, para el caso de los documentos, registrar el nombre asignado al documento de archivo o registro.
- **Descripción Del Activo De Información**: Realizar la descripción general del documento, especificando la información que contiene.
- **Idioma:** Establecer el Idioma, lengua o dialecto en que se encuentra la información consignada en el documento de archivo.

c. Tipo de Soporte (medio de conservación y/o soporte):

En la identificación del tipo de soporte, es importante definir el medio de conservación y/o soporte, así como el formato, lo cual se realizará en el formato Registro de Activos de Información.

- **Tipo De Activo**: Elegir de la lista desplegable, según corresponda: (Información, Hardware, Software, Servicio, Recurso Humano, Otros.)
- **Descripción Del Soporte:** Elegir de la lista desplegable según corresponda: (Tipo de soporte del activo de información, (Documento Físico, Documento Electrónico, Documento Digital, Documental Digital y Electrónico, Documento Físico y Electrónico, Documento Físico y Digital, Documento Físico, Digital y Electrónico, Otro)
- **Formato:** Identificar la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: (Animación Audio. Correo Electrónico, Documento de Texto, Correo Electrónico, Hoja de Cálculo, Compresión, Base de Datos, Documento de Texto, Hoja de Cálculo, Imagen, PDF, Presentaciones, Video, Web, Otro.)
- **Tipo De Origen**: Identificar dónde se genera la información contenida en el documento de archivo (interno/externo).

d. Clasificación Documental.

Se define como el listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos, es decir se considera como el Instrumento que permite establecer cuáles son los documentos de una Entidad, su necesidad e importancia en términos de tiempo de conservación y preservación y que debe hacerse con ellos una vez finalice su vigencia o utilidad.

- **Serie:** en este ítem se registra el nombre asignado en la tabla de retención documental para la serie.

- **Subserie**: en este ítem se registra el nombre asignado en la tabla de retención documental para la subserie.
- **Descripción de la serie (categoría de información):** hacer una breve descripción del contenido de la serie y subserie documental.

e. Clasificación y Custodia de la Información

Realizar la clasificación de la información de la Entidad conforme lo indican las leyes 1712 de 2014, y 1581 de 2012, el Modelo de Seguridad y Privacidad en la Guía de Gestión de Activos, el control 5.9 del Anexo A de la norma ISO27001:2022 y demás normatividad aplicable.

- **¿Tiene datos personales?:** Elige Si o No, si contiene datos personales de acuerdo con la ley 1581 de 2012.
- **Clasificación de la información:** Elija entre las opciones de Información Pública, Información pública clasificada, Información pública reservada, de acuerdo con Ley 1712 2014 "Ley de Transparencia y acceso a la Información Pública"
- **Custodio de la información:** Indicar la dependencia de acuerdo con la lista desplegable.
- **Estado de la información:** Indicar si la información está disponible, de acuerdo con la lista desplegable.
- **Ubicación del activo de información:** Indicar el archivo de gestión o el lugar donde reposa el original del documento de acuerdo con la lista desplegable.
- **Publicada (link página web):** Incluya el link de consulta del documento.
- **Propietario del activo:** Nombre de la dependencia responsable de la producción del documento, de acuerdo con la lista desplegable.

f. Índice de Información Clasificada y Reservada

Realizar la validación de información de los activos de información de la Entidad de acuerdo con lo establecido en el Art 40. Contenido del índice de Información Clasificada y Reservada del Decreto 103 DE 2015.

- **Fecha de Generación de la Información clasificada y Reservada:** Momento de la creación de documento.
- **Objetivo Legitimo de la excepción:** La identificación de la excepción que, dentro de las previstas en los artículos 18 y 19 de la Ley 1712 de 2014, cobija la calificación de información reservada o clasificada.

- **Fundamento Constitucional o legal:** señalando expresamente la norma, artículo, inciso o párrafo que la ampara.
- **Fundamento jurídico de la Excepción:** Mención de la norma jurídica que sirve como fundamento jurídico para la clasificación o reserva de la información**.**
- **Excepción Total o Parcial**: Según sea integral o parcial la calificación, las partes o secciones clasificadas o reservadas.
- **Fecha de calificación:** La fecha de la calificación de la información como re-servada o clasificada.
- **Plazo de la clasificación o reserva de información:** el tiempo que cobija la clasificación o reserva.

g. Infraestructuras Críticas Cibernéticas – ICC.

Identificar y reportar a las instancias y autoridades respectivas en el Gobierno Nacional si la Entidad posee Infraestructura Critica Cibernética -ICC. Teniendo en cuenta que su impacto o afectación podría superar alguno de los siguientes criterios: Impacto social, Impacto económico e Impacto ambiental, conforme a la Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia, Primera Edición del Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia.

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Ilustración 18 Modelo de Gestión de Riesgos de Seguridad Digital - MINTIC

h. Componente de Seguridad de la Información.

Evaluar la criticidad de los activos de la Secretaría Distrital de Seguridad, Convivencia y Justicia, clasificando el grado de importancia de cada Activo de información de acuerdo con la Confidencialidad, Integridad y Disponibilidad (Alta, Media Baja), para posteriormente realizar el análisis de riesgos que establezca la criticidad y una valoración adecuada en cada caso con base al resultado. Lo anterior de acuerdo con lo definido en el Anexo 4 “lineamientos para la gestión de riesgos de seguridad digital en Entidades públicas” del MinTIC.

Importancia del activo/Criticidad del Activo: Se calcula automáticamente, de acuerdo con los criterios seleccionados en la Confidencialidad, Integridad y Disponibilidad, teniendo en cuenta la siguiente tabla de valoración:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o más componentes (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta o media en al menos uno (1) de sus componentes
BAJA	Activos de información en los cuales la clasificación de la información en todos sus componentes es baja.

Tabla 9, Elaboración propia

El sistema de clasificación de los activos de información de la Entidad, de realiza de acuerdo con los principios de; Confidencialidad, Integridad y Disponibilidad. Asimismo, contempla el impacto que causaría la pérdida de alguno de estos, estableciendo criterios específicos para el tratamiento del activo de información.

Asimismo, en esta Política se definieron tres (3) niveles de importancia / criticidad de los activos de información, que permiten determinar el valor general del activo en la Entidad (es importante aclarar que los niveles pueden definirse a criterio de la Entidad): Alta, Media y Baja, con el fin identificar qué activos deben tratarse de manera prioritaria.

En ese orden de ideas, en la Entidad se tratarán los activos de información clasificados con importancia alta, en los cuales la clasificación de la información en dos (2) o todas las propiedades (Confidencialidad, Integridad, y Disponibilidad) es alta, acorde con el alcance definido para la implementación del Modelo de Seguridad y Privacidad de la Información alineadas con la gestión de activos – Control 5.9 – Inventario de información y otros activos asociados del anexo A de la norma ISO 27001:2022.

14.4 Identificación del riesgo

La Identificación del riesgo de seguridad de la Información en la Entidad, se realiza de acuerdo con lo definido en el Anexo 4 del Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades Públicas del Departamento Administrativo de la Función Pública- DAFP:

En el cual, se podrán identificar tres (3) riesgos inherentes de seguridad de la información: Pérdida de la confidencialidad, Pérdida de la integridad y Pérdida de la disponibilidad. En cada riesgo se deben asociar el grupo de activos, o activos

específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

a. **Identificación de los riesgos inherentes de seguridad de la información**

De acuerdo con lo definido en el anexo 4 de Lineamientos para la Gestión de Riesgos de Seguridad Digital - GRSD y complementadas por la Guía De Gestión De Riesgos emitida por el MinTIC, a través de la estrategia de Gobierno Digital para la Seguridad y privacidad de la información. A continuación, se detallan las amenazas comunes que pueden hacer daño a los activos de la Entidad, materializar los riesgos y generar algunas vulnerabilidades (debilidades):

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	**A, D, E**
	Agua	**A, D, E**
	Contaminación	**A, D, E**
	Accidente Importante	**A, D, E**
	Destrucción del equipo o medios	**A, D, E**
	Polvo, corrosión, congelamiento	**A, D, E**
Eventos naturales	Fenómenos climáticos	**E**
	Fenómenos sísmicos	**E**
	Fenómenos volcánicos	**E**
	Fenómenos meteorológicos	**E**
	Fenómenos Ambiental	**E**
	Inundación	**E**
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	**A, D, E**
	Perdida de suministro de energía	**E**
	Falla en equipo de telecomunicaciones	**A, D, E**
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 comprometida	**D**
	Espionaje remoto	**D**
	Escucha encubierta	**D**
	Hurto de medios o documentos	**D**
	Hurto de equipo	**D**
	Recuperación de medios reciclados o desechados	**D**
	Divulgación	**D**
	Datos provenientes de fuentes no confiables	**D**
	Manipulación con hardware	**D**
	Manipulación con software	**D**
	Detección de la posición	**D**
	Incumplimiento de la Divulgación	**D**
	Actividad Maliciosa de Ciberdelincuente	**D**
	Gestión Inadecuada de la Información	**D**
	Ciberataque	**D**
	Modificación de Base de Datos.	**D**
	Ciberataque o incidente informático a la infraestructura del proveedor de nube	**D**
	Ciberataque dirigido a la infraestructura de la Entidad	**D**
	Perdida de Información	**D**

TIPO	AMENAZA	ORIGEN
Fallas técnicas	Fallas del equipo	**D, E**
	Mal funcionamiento del equipo	**D, E**
	Saturación del sistema de información	**D, E**
	Mal funcionamiento del software	**D, E**
	Incumplimiento en el mantenimiento del sistema de información.	**D, E**
	Indisponibilidad de los Sistemas de Información	**D, E**
	Mantenimiento de Equipos Inadecuado	**D, E**
Acciones no autorizadas	Uso no autorizado del equipo o Software	**D, E**
	Copia fraudulenta del software	**D, E**
	Uso de software falso o copiado	**D, E**
	Corrupción de los datos	**D, E**
	Procesamiento ilegal de datos	**D, E**
	Uso no autorizado de credenciales de administración a cualquiera de los componentes de la infraestructura de la SDSCJ	**D, E**
Compromiso de las funciones	Error en el uso	**D, E**
	Abuso de derechos	**D, E**
	Abuso de derechos y corrupción de los datos	**D, E**
	Falsificación de derechos	**D**
	Negación de acciones	**D, E**
	Incumplimiento en la disponibilidad del personal	**D, E**

Tabla 10, ISO/IEC 27005:2009

D= Deliberadas, **A**= Accidentales, **E**= Ambientales

A continuación, se detallan las **Amenazas dirigidas por el hombre** empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla 11

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado Chantaje

Tabla 18, ISO/IEC 27005:2009

Las siguientes son las **vulnerabilidades comunes** las cuales se pueden identificar vulnerabilidades (debilidades), de acuerdo con el tipo de activo:

Tipos	Ejemplo de vulnerabilidad	Ejemplo de Amenaza
Hardware	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento.
	Ausencia de un eficiente control de cambios en la configuración.	Error en el uso
	Susceptibilidad a las variaciones de voltaje.	Pérdida del suministro de energía.
	Susceptibilidad a las variaciones de temperatura.	Fenómenos meteorológicos.
	Almacenamiento sin protección.	Hurto de medios o documentos.
	Falta de cuidado en la disposición final.	Hurto de medios o documentos.
	Copia no controlada.	Hurto de medios o documentos.
	No se cuenta con un mecanismo seguro y estandarizado de manejo de credenciales de administración a la infraestructura tecnológica	Abuso de derechos.
Software	Ausencia o insuficiencia de pruebas de software.	Abuso de derechos.
	Defectos bien conocidos en el software	Abuso de derechos.
	Ausencia de “terminación de la sesión” cuando se abandona la estación de trabajo.	Abuso de derechos.
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.	Abuso de derechos.
	Ausencia de pistas de auditoría.	Abuso de derechos.
	Asignación errada de los derechos de acceso.	Abuso de derechos.
	Software ampliamente distribuido.	Corrupción de datos.
	En término de tiempo utilización de datos errados en los programas de aplicación.	Error en el uso.
	Interfaz de usuario compleja.	Error en el uso.
	Ausencia de documentación.	Error en el uso.
	Configuración incorrecta de parámetros.	Error en el uso.
	Fechas incorrectas.	Error en el uso.
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario.	Falsificación de derechos.
	Tablas de contraseñas sin protección.	Falsificación de derechos.
	Gestión deficiente de las contraseñas.	Falsificación de derechos.
	Habilitación de servicios innecesarios.	Procesamiento ilegal de datos.
	Software nuevo o inmaduro.	Mal funcionamiento del software
	Especificación incompleta o no clara para los desarrolladores.	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software.
	Descarga y usos no controlados de software.	Manipulación de software.
	Ausencia de copias de respaldo.	Manipulación de software.
	Ausencia de protección física de la edificación, puertas y ventanas.	Hurto de medios o documentos.
	Falla en la producción de informes de gestión.	Uso no autorizado del equipo.
	Ausencia y/o alteración de documentación.	Manipulación de software
	Ausencia de guías para el adecuado uso de la plataforma	Error en el uso.
	Acceso y uso inadecuado de la información	Manipulación de software
	Registro de información no verificada	Manipulación de software

Tipos	Ejemplo de vulnerabilidad	Ejemplo de Amenaza
	Dificultad para la verificación de los datos registrados	Error en el uso.
	Obsolescencia y brechas de seguridad por uso de versionamiento desactualizado del entorno de desarrollo de los diferentes sistemas de información.	Error en el uso.
	Falta de Arquitectura de datos estandarizada para los sistemas de información	Error en el uso.
Red	Ausencia de pruebas de envío o recepción de mensajes.	Negación de acciones.
	Líneas de comunicación sin protección.	Escucha encubierta.
	Tráfico sensible sin protección.	Escucha encubierta.
	Conexión deficiente de los cables.	Falla de equipo de telecomunicaciones.
	Punto único de falla.	Falla de equipo de telecomunicaciones.
	Ausencia de identificación y autentificación de emisor y receptor.	Falsificación de derechos.
	Arquitectura insegura de la red.	Espionaje remoto.
	Transferencia de contraseñas en claro.	Espionaje remoto.
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información.
	Conexiones de red pública sin protección de control de acceso.	Uso no autorizado del equipo.
Personal	Ausencia del personal.	Incumplimiento en la disponibilidad del personal
	Procedimiento inadecuado de contratación.	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad.	Error en el uso.
	Uso incorrecto de software y hardware.	Error en el uso.
	Falta de conciencia acerca de la seguridad.	Error en el uso.
	Ausencia de mecanismos de monitoreo.	Procesamiento ilegal de los datos.
	Trabajo no supervisado del personal externo o de limpieza.	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	Hurto de medios o documentos.
	Rotación del Personal	Error en el uso.
	Datos provenientes de fuentes no confiables	Error en el uso.
	Respuesta Inadecuada de mantenimiento del servicio	Error en el uso.
	Falta de control periódico sobre los derechos de acceso.	Abuso de derechos.
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios.	Abuso de derechos.
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.	Abuso de derechos.

Tipos	Ejemplo de vulnerabilidad	Ejemplo de Amenaza
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes.	Abuso de derechos.
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información.	Abuso de derechos.
	Ausencia de auditorías (supervisiones) regulares.	Abuso de derechos.
	Ausencia de procedimiento de identificación y valoración de riesgos	Abuso de derechos.
	Ausencia de procedimientos de identificación de valoración de riesgos.	Abuso de derechos.
	Ausencia de reportas de fallas en los registros de administradores y operadores.	Abuso de derechos.
	Respuesta inadecuada de mantenimiento del servicio.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimiento de control de cambios.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimiento formal para el control de la documentación del SGSI.	Corrupción de datos.
	Ausencia de procedimiento formal para la supervisión del registro del SGSI.	Corrupción de datos.
	Ausencia de procedimiento formal para la autorización de información disponible al público.	Datos provenientes de fuentes no confiables.
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información.	Negación de acciones.
	Ausencia de planes de continuidad.	Falla del equipo.
	Ausencia de políticas sobre el uso del correo electrónico.	Error en el uso.
	Ausencia de procedimientos para la introducción del software en los sistemas operativos.	Error en el uso.
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso.
	Ausencia de procedimientos para el manejo de información clasificada.	Error en el uso.
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos.	Error en el uso.
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con loe empleados.	Procesamiento ilegal de datos.
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información.	Hurto de equipo.
	Ausencia de política formal sobre la utilización de computadores portátiles.	Hurto de equipo.
	Ausencia de control de los activos que se encuentran fuera de las instalaciones.	Hurto de equipo.
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla.	Hurto de medios o documentos.
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad.	Hurto de medios o documentos.

Tipos	Ejemplo de vulnerabilidad	Ejemplo de Amenaza
	Ausencia de revisiones regulares por parte de la gerencia.	Hurto de medios o documentos.
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.	Hurto de medios o documentos.
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falso o copiado.

Tabla 12 ISO/IEC 27005:2009

Las siguientes son las **consecuencias** más comunes que pueden afectar a la Entidad de forma directa o indirecta y que pueden afectar la operación de la misma:

Consecuencias
Cancelación de la licencia de funcionamiento
Daño en los activos
Deficiencias o deterioro del servicio al ciudadano
Demandas, litigios, derechos de petición o tutelas
Demoras en los servicios prestados y ejecución de los procesos
Interrupción de los sistemas / procesos
Multas o sanciones
Pérdida de clientes
Pérdida de confianza del ciudadano
Pérdida de reputación y/o de imagen
Pérdida de vidas
Pérdida o detrimento de información
Pérdidas de conocimiento
Pérdidas económicas
Reclamaciones o quejas de ciudadanos

Tabla 13 ISO/IEC 27005:2009

Es importante tener en cuenta que, una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control. En la siguiente tabla se representan los ejemplos de vulnerabilidades y amenazas respecto al tipo de Activo.

Tipo de activo	Ejemplos de Vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos

Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Tabla 14 ISO/IEC 27005:2009

14.5 Valoración del riesgo

La valoración del riesgo de seguridad de la Información en la Secretaría Distrital de Seguridad, Convivencia y Justicia se ajusta de acuerdo con lo establecido en el **numeral 9.6** de la presente Política apropiando lo indicado en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" Versión 6 – 2022 del Departamento Administrativo de la Función Pública **DAFP.**

Lo anterior, permite establecer la probabilidad y las consecuencias por la posible materialización de los riesgos para la Entidad, siendo necesario determinar las tasas de probabilidad que se definen en la siguiente tabla:

Nivel de Probabilidad	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 1 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 2 a 1.000 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 1.001 a 5.000 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 5.001 veces al año y máximo 10.000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 10.001 veces por año	100%

Tabla 15 Valoración riesgos de seguridad de la información
Oficina Asesora de Planeación Secretaría Distrital de Seguridad, Convivencia y Justicia.

De igual forma para determinar el impacto económico y reputacional se cuenta con la siguiente tabla que es valorada por niveles de la siguiente forma:

Niveles de Impacto	Afectación Económica	Afectación Reputacional	Impacto
Leve	Afectación menor a 49.999 SMLMV	El riesgo afecta la imagen de algún área de la organización.	20%
Menor	Entre 50.000 y 99.999 SMLMV	El riesgo afecta la imagen de la Entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	40%
Moderado	Entre 100.000 y 199.999 SMLMV	El riesgo afecta la imagen de la Entidad con algunos usuarios de relevancia frente al logro de los objetivos.	60%

Niveles de Impacto	Afectación Económica	Afectación Reputacional	Impacto
Mayor	Entre 200.000 y 299.999 SMLMV	El riesgo afecta la imagen de la Entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	80%
Catastrófico	Mayor a 300.000 SMLMV	El riesgo afecta la imagen de la Entidad a nivel nacional, con efecto publicitario sostenido a nivel país	100%

Tabla 16 impacto económico y reputacional
Oficina Asesora de Planeación Secretaría Distrital de Seguridad, Convivencia y Justicia.

Siendo determinada los criterios de probabilidad **(P)** y a su vez los criterios de impacto **(I)** del evento de riesgo de seguridad de la información en la Entidad, se obtiene el nivel de riesgo inherente ubicando la posición de acuerdo con la valoración obtenida de cada variable P e I en el siguiente plano cartesiano (Mapa de calor):

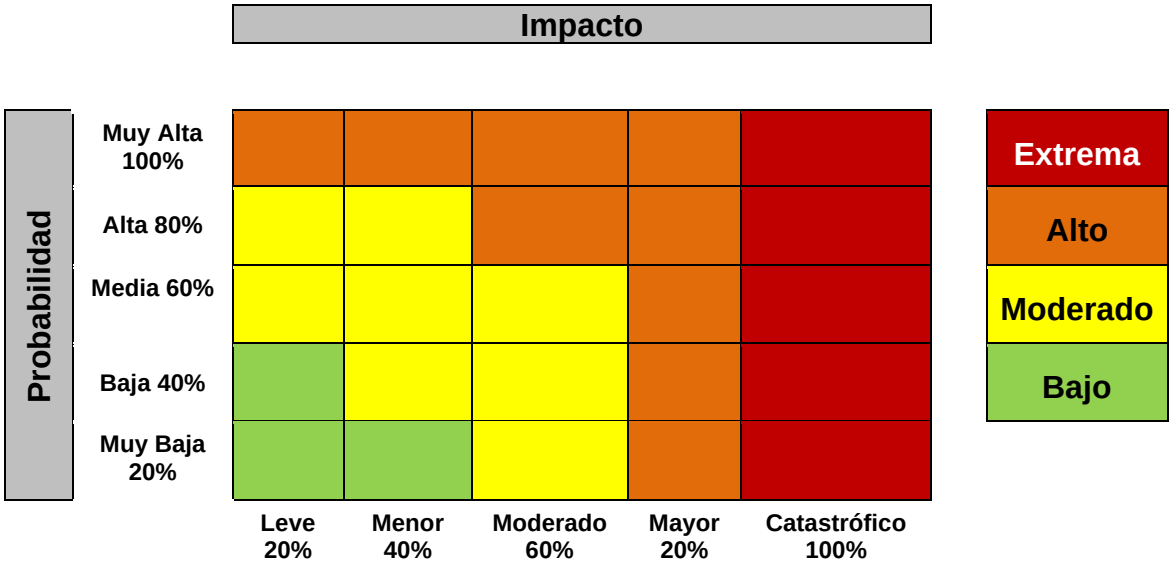

Tabla 17 Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas. Ver. 6

Si el nivel del riesgo inherente es **bajo**, el líder del proceso puede tomar la decisión de aceptar el riesgo y no será necesaria la implementación de una medida de mitigación, en otras palabras, la Entidad solo tendrá un Nivel de Apetito al riesgo **bajo.**

Por otro lado, si el nivel de riesgo inherente es diferente a **bajo**, obligatoriamente se debe implementar una medida de mitigación o reducción para el **riesgo** *(implementar un control)*. a reducir el riesgo (implementar un control), evitar el riesgo *(dejar de realizar la actividad con la cual está relacionada el riesgo*) o compartir el riesgo (*transfiriéndolo o compartiéndolo con un agente externo al proceso implementando un control).*

Cabe resaltar que la Oficina Asesora de Planeación independiente de la Zona de Calor recomienda la estructuración de controles para evitar materializaciones y consecuentemente futuros cambios en la zona de calor.

Tratamiento del riesgo de Seguridad de la Información

En esta etapa la primera línea de defensa (líderes de procesos) determinan, tomando en cuenta cual es el nivel del riesgo inherente, que acción es la más adecuada para su tratamiento, estas acciones pueden ser:

- **Aceptar el riesgo:** Valido únicamente para aquellos cuya Zona de Riesgo Residual es **Baja** no se aplica ninguna acción adicional a la ejecución permanente del control que se tiene estipulado asumiendo el mismo conociendo los efectos de su posible Materialización.
- **Reducir el riesgo:** Para aquellos cuya Zona de Riesgo Residual sea diferente a **Baja**, se deberán toman acciones mediante Transferencia o Mitigación previa realización de un análisis de la situación dejando evidencia en la Matriz de Riesgos:
    - **Mitigar:** Esto se logra por medio de acciones que mitiguen el nivel de Riesgo, no necesariamente se refiere a la implementación de controles adicionales.
    - **Transferir:** Estrategia de tercerización del proceso o traslado del riesgo a través de Seguros o Pólizas. La Responsabilidad económica recaerá sobre el tercero. Sin embargo, se mantiene la Responsabilidad reputacional.
- **Evitar el riesgo:** Se determina no asumir el riesgo por lo cual se elimina la ejecución de las actividades que faciliten la materialización

Si el líder del proceso decide que la acción de tratamiento al evento de riesgo será la de **reducir el riesgo o compartir el riesgo** se debe diseñar una actividad de control, la cual podrá ser diseñada por el líder operativo, pero debe tener el aval del líder del proceso.

14.6 Creación de Controles

Los Controles en Seguridad de la Información se definen como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta lo siguiente:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o profesionales designados.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Para que un control este adecuadamente diseñado y que su implementación sea efectiva a la hora de mitigar un riesgo, se crea de acuerdo con los lineamientos descritos en el **numeral 9.7** creación de controles del presente documento.

14.7 Tratamiento del Riesgo Residual

Dada la Zona de Riesgo Residual obtenida con la ejecución de controles, se realiza un tratamiento a los riesgos identificados que se aplica de la siguiente forma:

- **Aceptar el riesgo:** Valido únicamente para aquellos cuya Zona de Riesgo Residual es **Baja** no aplicara ninguna acción adicional a la ejecución permanente del control que se tiene estipulado.
- **Reducir el riesgo:** Para aquellos cuya Zona de Riesgo Residual sea diferente a **Baja**, se deberán toman acciones adicionales para disminuir la probabilidad y/o el impacto, esto se logra por medio de la implementación de controles adicionales que deberán analizarse dentro de un periodo de tiempo, cuyo limite es la finalización del Año que se encuentre en curso y dependiendo del resultado deberán incluirse como Controles para el siguiente Año.
- **Evitar el riesgo:** Se elimina la ejecución de las actividades que facilitan la materialización del riesgo.
- **Compartir el riesgo:** Para aquellos cuya Zona de Riesgo Residual sea diferente a **Baja**, se busca disminuir el impacto y/o la probabilidad del riesgo compartiéndolo con otro proceso de la Entidad o con un actor tercero, por ejemplo, mediante una póliza de seguro con una compañía exógena a la Entidad que deberán ser analizados dentro de un periodo de tiempo, cuyo limite es la finalización del Año que se encuentre en curso y dependiendo del resultado deberán ser incluidos como Controles para el siguiente Año.

Todos los riesgos deben contar con algún tratamiento residual independiente de la Zona de Riesgo, únicamente están permitidas las actividades anteriormente descritas.

14.8 Monitoreo, revisión y reporte

Consiste en la permanente evaluación que permita asegurar que dicha gestión se está llevando a cabo bajo los aspectos y lineamientos definidos por la Entidad para los riesgos de seguridad de la información.

1. El Mapa de riesgos de seguridad de la información, debe contener aquellas acciones de control definidas para el manejo del riesgo, buscando prevenir o reducir el riesgo detectado, teniendo en cuenta su viabilidad técnica y financiera. El monitoreo de las acciones de tratamiento debe realizarlo el responsable del proceso.
2. El responsable del proceso debe verificar que los controles establecidos en la matriz de riesgos operen de manera adecuada para mitigar los riesgos.
3. El seguimiento de los riesgos identificados (incluyendo el tratamiento) se debe realizar de manera cuatrimestral por cada uno de los líderes de los procesos, quienes reportarán a la Dirección de Tecnologías y Sistemas de la Información quien consolidará y posteriormente enviará a la Oficina Asesora de Planeación para su publicación.
4. Anualmente se debe realizar la valoración de los riesgos de seguridad de la información con el fin de verificar que el tratamiento fue efectivo y los niveles de riesgo disminuyeron.
5. El responsable de realizar el seguimiento a los riesgos de seguridad de la Información debe reportar cuatrimestralmente a la mesa técnica de Seguridad Digital.

15 IDENTIFICACIÓN Y GESTIÓN DE RIESGOS ESTRATÉGICOS

Los Riesgos Estratégicos surgen del ejercicio de Planeación Estratégica y parten directamente de los Objetivos Estratégicos para cumplir satisfactoriamente con el fin de la correcta administración del riesgo, se hace necesario seguir las siguientes etapas detalladamente. Se enfatiza en el objetivo de identificar, analizar, dar tratamiento, finalizando con el seguimiento y evaluación a los riesgos. Con ello se logra una visión integral de las actividades propias de la Entidad que podrían afectar el cumplimiento de las metas y objetivos trazados. Aplicar formato Matriz de Riesgos Estratégicos F-FI-1479.

15.1 Etapa 1: Conocimiento y Divulgación

La presente Política debe ser de conocimiento general para los funcionarios directos e indirectos de la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, se debe tener en cuenta que en este documento se especifican los lineamientos técnicos con los cuales se ejecutara la gestión del riesgo en la Entidad, por ende toda persona que interactúe con procesos y procedimientos debe actuar activamente en atención a la Gestión del Riesgo, considerando su conocimiento, punto de vista, percepciones y experiencia, propendiendo la mejor decisión evitando las posibles afectaciones y consecuencias por el desarrollo de actividades.

La Matriz es publicada en la página WEB e intranet en las siguientes rutas:

WEB: https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, Presupuesto e Informes - Plan de acción - Planes Estratégicos, Sectoriales e Institucionales - Plan Estratégico Institucional

15.2 Identificación y tratamiento de Riesgos

El ejercicio se realiza partiendo de cada uno de los Objetivos Estratégicos estructurados y se procede con la identificación de los siguientes aspectos de forma individual:

- Proceso(s) responsables.
- Amenazas y Debilidades asociadas de acuerdo con la Matriz DOFA de la Entidad la cual debe actualizarse en el ejercicio de Planeación Estratégica.
- Mediante el Metalenguaje identificar (debido a – Podría suceder – lo que generaría) Riesgo y consecuencias teniendo en cuenta que las Amenazas y Debilidades serán las causas.
- El nivel de Riesgo Inherente será para todos "**Extremo**" teniendo en cuenta que corresponde a los Objetivos estratégicos.
- Como tratamiento todos tendrán que contemplarse como "Reducir el Riesgo" (implementar un control) para el nivel de Riesgo Inherente. Para el nivel de Riesgo Residual se contempla la formulación de Planes de acción de ser necesarios.
- Los controles deben ser preventivos deben contar con la siguiente estructura:
  - ✓ Debe tener un **responsable** de su ejecución (evitar colocar áreas generales o nombres propios), por ejemplo: responsable de inventarios.
  - ✓ La ejecución del control **debe tener un soporte documental**, por ejemplo, una base de datos, una lista de chequeo, un acta de reunión, etc.
  - ✓ En la descripción del control se debe **especificar como se ejecuta** el control,

- ✓ En la definición del control se debe especificar cuál es la **periodicidad de la aplicación** de este; por ejemplo: *el coordinador debe revisar (mensualmente, trimestralmente, cada vez que se presente…)*
- ✓ La definición debe incluir **cual es el propósito** del control (valida, coteja, compara, concilia…)
- ✓ La definición del control debe incluir en que situaciones se presentan **desviaciones entre el resultado esperado y el resultado obtenido** y que acciones se deben tomar si se presentan dichas desviaciones.

- Se les efectuará la Calificación a los controles de acuerdo con lo establecido en el **numeral 12.8**
- El ejercicio culminará con estructura del indicador de cumplimiento.

15.3 Nivel de Riesgo residual

Con el resultado de la evaluación se determina la Zona de Riesgo Residual de acuerdo con lo establecido en el **numeral 12.9**.

15.4 Tratamiento del Riesgo Residual

Se acepta el Riesgo residual teniendo en cuenta que las actividades generadoras del Riesgo hacen parte de la misionalidad de la Entidad y por ende no pueden evitarse ni transferirse, se realiza seguimiento de acuerdo con lo establecido en la Política de Administración de Riesgos, efectuando los ajustes que se consideren necesarios para cumplir con los objetivos de la Entidad.

16 IDENTIFICACIÓN Y GESTIÓN DEL RIESGO FISCAL

Partiendo de la “Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas” el presente numeral tiene como finalidad prevenir el posible daño al patrimonio público, representando menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

Recordando que la responsabilidad fiscal está consignada en la Ley 610 de 2000. Las cuales están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, modificadas por el Acto Legislativo 04 de 2019 fundamentado en la necesidad de un ejercicio preventivo del control fiscal, que detenga el daño fiscal e identifique los riesgos fiscales en la Entidad; con ello, la Línea Estratégica podrá adoptar las

medidas necesarias para prevenir la concreción del daño patrimonial de naturaleza pública.

El riesgo Fiscal se define como el "Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial", en el cual surge de los daños que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial, este último corresponde a los hechos inciertos o incertidumbres, con una potencial acción u omisión que podrían generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública; también se entiende el evento potencial como la causa raíz del Riesgo.

Para cumplir satisfactoriamente con el objetivo de la correcta administración del riesgo, se hace necesario seguir las siguientes etapas detalladamente. Se enfatiza en el objetivo de identificar, analizar, dar tratamiento, finalizando con el seguimiento y evaluación a los riesgos, logrando una visión integral de las actividades propias de la Entidad que podrían afectar el cumplimiento de las metas y objetivos trazados.

16.1 Apetito, Tolerancia y Capacidad del Riesgo Fiscal

Para el Apetito del Riesgo, Tolerancia del Riesgo y Capacidad del riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión de Integridad definidos anteriormente

16.2 Identificación del Riesgo

Para la identificación del riesgo fiscal es necesario establecer los **puntos de Riesgo Fiscal** que corresponde a las situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas. O anterior indica que son todas las actividades que representan Gestión Fiscal contemplando aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Complementando el ejercicio de los puntos de Riesgo se deben identificar las **circunstancias inmediatas**, siendo aquellas situaciones o actividades bajo la cual se presenta el riesgo, pero no constituyen la causa principal o causa raíz para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas. Para mantener unificado el criterio de

identificación del Riesgo la **Circunstancia Inmediata** corresponde a la **Causa Inmediata** definida para los Riesgos de Gestión.

16.3 Identificación de Puntos de Riesgo Fiscales y Causa Inmediata

Para lograr una adecuada estructuración se desarrolla el siguiente ejercicio:

- **Taller de Identificación:** Realización de taller con los lideres de Procesos u Operativos, en compañía de los asesores y servidores que se consideren necesarios por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de gestión fiscal en las que potencialmente se genera riesgo fiscal) y Causas Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal). En el taller, se formulan las siguientes preguntas:

  - ✓ ¿En qué procesos de la Entidad se realiza gestión fiscal?
  - ✓ ¿Cuáles son los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal relacionados con hechos de la Entidad y las advertencias recibidas por Contraloría de Bogotá o la oficina de control interno, en los últimos 5 años?

- **Análisis del Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas:** El Departamento Administrativo de la Función Pública estructuró el “CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS” el cual suministra como Anexo 1 de la “Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas” en su versión 6, a continuación, se enuncian los puntos de Riesgo y las Circunstancias (Causas) inmediatas. Que pueden generar un efecto al patrimonio Público.

Id	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Causa Inmediata** *Situación **por la que** se presenta el riesgo*
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la Entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la Entidad	Saldos o recursos a favor no cobrados

Id	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Causa Inmediata** *Situación **por la que** se presenta el riesgo*
6	Custodiar de los bienes muebles de la Entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la Entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la Entidad	Daño en bienes muebles de propiedad de la Entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la Entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la Entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron asignarse al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la Entidad- todos los bienes muebles e inmuebles de la Entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad

Id	**Puntos de Riesgo Fiscal** *Actividad en la que potencialmente se origina el riesgo fiscal*	**Causa Inmediata** *Situación **por la que** se presenta el riesgo*
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas a los contratistas
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la Entidad o pagos por parte de deudores	Reintegro de saldos a favor de la Entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la Entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la Entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Tabla 23, Anexo 1: Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas.

Los ejercicios antes descritos deben efectuarse como mínimo una vez al año y deben respaldarse con Actas de reunión con los Lideres de Proceso u Operativos.

El ejercicio se respalda con la verificación de matriz de Plan de mejoramiento de Contraloría de la Entidad y la asesoría de la Oficina de Control Interno.

16.4 Identificación de la Causa Raíz o Potencial Hecho Generador

La causa raíz o potencial hecho generador es aquel evento potencial (acción u omisión) que provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño/Impacto) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio.

Para mantener la adecuada Gestión del Riesgo se exige que la identificación de causas sea objetiva y rigurosa, permitiendo ya que los controles que se diseñen e implementen apunten a atacar las causas, para así lograr prevenir la ocurrencia de daños fiscales.

16.5 Estructuración del Riesgo Fiscal

Como parte fundamental en la Gestión del Riesgo, este se debe formular y redactar adecuadamente para lograr un entendimiento y tratamiento pertinente. Por lo anterior y tomando lo información del numeral anterior para redactar un riesgo fiscal se debe tener en cuenta:

✓ Iniciar con la oración: **Posibilidad de**, debido a que nos estamos refiriendo al evento potencial.
✓ Impacto: Corresponde al **qué**. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
✓ Causa (Circunstancia) inmediata: Corresponde al **cómo**. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
✓ Causa Raíz: Corresponde al **por qué**; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.
De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:

Dado lo anterior, la siguiente será la estructura del Riesgo partiendo del Impacto y lo mencionado en la Etapa 4:

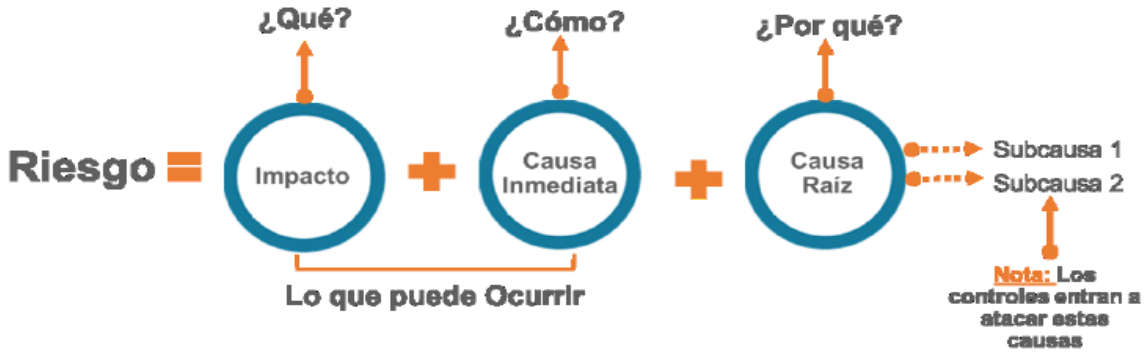

Ilustración 22. Estructura Riesgo Fiscal
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas

La descripción del riesgo debe contener todos los detalles antes ilustrados con la intención de que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. La estructura facilita su redacción y claridad, 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.

La redacción siempre debe iniciar con la frase POSIBILIDAD DE. De acuerdo con lo anterior, todos los Riesgos deben redactarse con la siguiente estructura:

Ilustración 23. Ejemplo Riesgos Fiscales

Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas

Los siguientes son ejemplos de Riesgos Fiscales.

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

Tabla 24. Ejemplos
Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas

16.6 Valoración del riesgo de Gestión

En adelante los Riesgos Fiscales se administran con la metodología impartida para los Riesgos de Gestión, en este caso aplica lo indicado en el **numeral 11.6.**

16.7 Creación de Controles

Para la creación de controles del riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el **Numeral 11.7** del presente documento.

16.8 Calificación del control

Para la Calificación del control del riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el **Numeral 11.8** del presente documento.

16.9 Nivel de Riesgo Residual

Para determinar el Nivel de Riesgo residual del riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el **Numeral 11.9** del presente documento.

Los periodos de corte para la entrega de evidencias y posterior elaboración de informe son indicados en la Política de Administración de Riesgos.

16.10 Tratamiento del Riesgo Residual

El Tratamiento del Riesgo residual del riesgo fiscal se toman los lineamientos definidos para los Riesgos de Gestión en el **Numeral 11.10** del presente documento.

17 IDENTIFICACIÓN Y GESTIÓN DE OPORTUNIDADES

De acuerdo con los lineamientos establecidos en la ISO 9001:2015, las Entidades deben establecer acciones para abordar los riesgos y oportunidades, para el primero de los casos, es decir los **riesgos** es necesario tener en cuenta que se presenta para aquellos casos que pueden generar una afectación de carácter potencialmente negativo (aspectos que han sido abordados en los numerales anteriores); **las oportunidades** se entienden como aquellas situaciones, condiciones o factores que, de materializarse y ser gestionados de manera adecuada, pueden generar beneficios, mejoras o fortalecimiento del desempeño institucional, contribuyendo al cumplimiento de los objetivos, a la optimización de los procesos y a la generación de valor público.

De acuerdo con lo enunciado, el tratamiento de oportunidades atenderá de manera secuencial una serie de etapas, para lo cual el documento referente será la **Matriz de identificación, calificación y seguimiento de oportunidades institucionales F-FI-1383**, la cual se describe a continuación:

17.1 Identificación de Oportunidades

Las fuentes para la identificación de oportunidades serán el Analisis de Contextos, la matriz DOFA, la Planeación Estratégica, la Actualización de Riesgos, los informes de Revisión por la Dirección, compromisos y/o recomendaciones del CIGD o CICCI, Lecciones Aprendidas o Informe de Mapa de Aseguramiento.
Es importante que el proceso realice una valoración de cuales de las oportunidades son relevantes para ser registradas en la matriz de oportunidades F-FI-1383.

17.2 Justificación

Se define como el efecto positivo o el beneficio o resultado favorable y verificable que se prevé obtener al aprovechar e implementar la oportunidad, reflejado en la mejora del desempeño institucional o del proceso, el cumplimiento de los objetivos y metas, la optimización de recursos, el fortalecimiento de la calidad del servicio y/o la generación de valor para la Entidad y sus grupos de valor.

17.3 Evaluación De Oportunidades

Las oportunidades se califican a través de viabilidad y factibilidad, para ello se entenderá por cada uno lo siguiente:

Viabilidad: Es la evaluación que determina si la oportunidad puede implementarse en la Entidad, considerando la disponibilidad y suficiencia de condiciones técnicas, financieras y jurídicas, así como las restricciones institucionales y normativas para su desarrollo, de acuerdo con los criterios definidos a continuación:

Viabilidad	Calificación	Descripción
Seguro	5	El proceso dispone plenamente de los recursos técnicos, financieros, jurídicos y de talento humano necesarios para la implementación de la oportunidad. Existen capacidades institucionales consolidadas y apoyo directivo para su ejecución. Probabilidad de logro entre 80% y 100%.
Muy Probable	4	El proceso cuenta con la mayoría de los recursos requeridos, aunque puede requerir apoyo o coordinación con otras dependencias o entidades. Existen condiciones favorables para su desarrollo y gestión. Probabilidad de logro entre 60% y 80%.

Viabilidad	Calificación	Descripción
Probable	3	El proceso presenta capacidades parciales para implementar la oportunidad; dispone de algunos recursos o competencias, y puede gestionar los faltantes mediante planeación o apoyo interinstitucional. Probabilidad de logro entre 40% y 60%.
Poco Probable	2	El proceso tiene limitaciones significativas de recursos, tiempo o competencias, aunque podría ejecutarse parcialmente con acompañamiento externo. Probabilidad de logro entre 20% y 40%.
Improbable	1	El proceso no cuenta con los recursos, competencias o condiciones normativas necesarias para implementar la oportunidad, ni se prevé la posibilidad de adquirirlos en el corto plazo. Probabilidad de logro entre 0% y 20%.

Tabla 18. Escala de Calificación Viabilidad de la Oportunidad
Fuente: Oficina Asesora de Planeación SDSCJ

Factibilidad: Es la estimación y verificación del beneficio real o potencial que se obtiene al implementar la oportunidad, en términos de generación de valor para la Entidad (mejora del desempeño, cumplimiento de objetivos, eficiencia, calidad del servicio, fortalecimiento institucional y/o impacto en grupos de valor), de acuerdo con los criterios definidos a continuación:

Factibilidad	Calificación	Descripción
Alto	5	La implementación de la oportunidad genera mejoras significativas en la gestión institucional y contribuye directamente al cumplimiento de los requisitos legales, técnicos y de los usuarios internos o externos. Se fortalece la eficiencia, la calidad del servicio y la satisfacción de las partes interesadas.
Medio	3	La implementación de la oportunidad mejora parcialmente las condiciones operativas del proceso, generando avances en tiempos, recursos o cumplimiento de algunos requisitos, sin un cambio estructural del desempeño institucional.
Baja	1	La implementación de la oportunidad no genera un cambio relevante en la operación del proceso, ni contribuye de manera significativa al cumplimiento de los requisitos o a la satisfacción de los usuarios y partes interesadas.

Tabla 19. Escala de Calificación Factibilidad de la Oportunidad

Fuente: Oficina Asesora de Planeación SDSCJ

17.4 Potencial de Aprovechamiento

Nivel resultante del cruce entre la viabilidad y la factibilidad de una oportunidad, que indica la conveniencia y prioridad de su aprovechamiento por parte de la Entidad; el potencial de aprovechamiento no se evalúa de manera aislada, sino como un resultado comparativo que permite identificar oportunidades con alta capacidad de implementación y alto beneficio, diferenciándolas de aquellas que, aunque viables, generan bajo valor, o que, aun siendo altamente beneficiosas, no cuentan con condiciones institucionales suficientes para su desarrollo.

Rango de Calificación		Nivel	Interpretación
13	**25**	Alta	La oportunidad es altamente viable y genera beneficios institucionales significativos. Su implementación debe priorizarse por el alto impacto en el cumplimiento misional, la eficiencia de los procesos o la satisfacción ciudadana.
6	**12**	Media	La oportunidad presenta condiciones favorables moderadas para su implementación. Se recomienda analizar su factibilidad y planear acciones graduales para su aprovechamiento, considerando recursos y prioridades institucionales.
1	**5**	Baja	La oportunidad tiene bajo potencial de beneficio o limitada viabilidad. Puede mantenerse en observación o reconsiderarse en futuros ciclos de planeación o mejora continua.

Teniendo en cuenta el nivel de potencial de aprovechamiento se deberán establecer los siguientes plazos de ejecución:

- ✓ Si el potencial de aprovechamiento presenta un nivel bajo, la estrategia de aprovechamiento debe desarrollarse en un plazo mayor a tres años o se debe tomar la decisión de inactivarla.
- ✓ Si el potencial de aprovechamiento presenta un nivel medio, la estrategia de aprovechamiento debe desarrollarse en largo plazo, es decir entre dos años y tres años.

- ✓ Si el potencial de aprovechamiento presenta un nivel alto, la estrategia de aprovechamiento debe desarrollarse en mediano plazo, es decir entre un año y dos año.

17.5 Estrategia de Aprovechamiento

Conjunto de acciones planificadas y coherentes orientadas a materializar la oportunidad identificada, asegurando que su implementación sea viable y genere los beneficios esperados para el cumplimiento de los objetivos institucionales o del proceso.

Estrategia de Aprovechamiento							
Actividad a realizar	¿ La actividad es financiera, tecnica y juridicamente viable?	Responsable	Fecha Inicio de Ejecución	Fecha límite de Ejecución	Evidencia	Verificación ¿Hay éxito post implementación? ¿Cuál?	Estado

Tabla 20. Estrategia de Aprovechamiento
Fuente: Oficina Asesora de Planeación SDSCJ

Nota 1: Las fechas en las cuales se desarrollarán las actividades, se relacionarán en el formato DD/MM/AA, se recomienda que este período corresponda al escenario de intervención de la oportunidad o la proyección del desarrollo de actividad descrita.
Nota 2: La evidencia es el producto verificable que demuestra la ejecución de la actividad.
Nota 3: El seguimiento es un reporte de avance en la ejecución de la oportunidad si ésta se encuentra en estado ***medio*** o ***alto***, de lo contrario diligenciar un reporte de ejecución total y reporte de la columna "verificación".

18 MONITOREO, EVALUACIÓN, AUDITORÍA, MEJORA CONTINUA Y PUBLICACIÓN.

El monitoreo y seguimiento de los riesgos constituye un proceso continuo que permite verificar la evolución de los riesgos identificados, la efectividad de los controles implementados y la ocurrencia de eventos que puedan afectar el cumplimiento de los objetivos institucionales.

Este proceso se desarrolla bajo el enfoque de las líneas de defensa, garantizando la trazabilidad de la información, la oportunidad en la toma de decisiones y la mejora continua del sistema de gestión del riesgo.

La versión vigente de las matrices será la última publicada en la Página WEB de la SDSCJ. Las matrices deben ser publicadas y divulgadas en la página web de la Entidad junto con los informes de seguimiento en el espacio de Transparencia y Acceso a la Información Pública.

Los resultados de la gestión del riesgo serán sociabilizados con los colaboradores de los equipos de trabajo en los diferentes comités o espacios institucionales que defina la entidad, deben ser periódicos, y en ningún caso deben superar un trimestre. No obstante, los resultados de los Informes de Seguimiento y evaluación de los riesgos serán sociabilizados y divulgados en el Comité de Gestión y Desempeño cada vez que sea pertinente.

18.1 Seguimiento y reporte

Los lideres de proceso son los responsables de la actualización permanente y documentación de los riesgos identificados. Garantizan que se realice permanentemente el seguimiento a los riesgos, lo que incluye:

- La evolución del riesgo (probabilidad e impacto)
- La efectividad de los controles implementados
- La materialización de eventos de riesgo
- La implementación de acciones de tratamiento
- Los indicadores claves asociados al riesgo

Este seguimiento debe realizarse de manera continua y documentarse en las herramientas definidas por la entidad.

- ✓ **Periodicidad:** Permanente
- ✓ **Responsable:** Procesos (Primera Línea de Defensa)
- ✓ **Alcance:** Monitoreo continuo y actualización de la información de riesgos

18.2 Monitoreo institucional

El reporte para el monitoreo de la segunda línea de defensa de los riesgos que hacen parte de la presente guía se realizará cuatrimestralmente para cada vigencia, y debe incluir entre otros:

- Validación de la adecuada identificación y valoración de riesgos
- Verificación de la coherencia entre riesgos, causas, controles y acciones
- Revisión de la calidad de la información reportada por los procesos

- Seguimiento a la efectividad de los controles
- Identificación de alertas, tendencias y riesgos emergentes

✓ **Periodicidad:** Cuatrimestral
✓ **Responsable:** Oficina Asesora de Planeación / Dirección de Tecnologías de la Información (Segunda Línea de Defensa)
✓ **Destino:** Comité Institucional de Gestión y Desempeño – CIGD

18.3 Reporte extraordinario

Se deberá realizar reporte inmediato cuando:

- Se materialice un riesgo
- Se identifiquen riesgos de alto impacto
- Existan eventos asociados a corrupción, fraude, LA/FT/FP o integridad
- Se presenten incidentes tecnológicos críticos
- Se generen afectaciones a recursos públicos o a la prestación del servicio.

18.4 Trazabilidad y evidencia

Toda la información relacionada con el monitoreo y reporte de riesgos y los respectivos controles debe:

- Estar documentada en las herramientas institucionales
- Contar con soportes verificables
- Garantizar consistencia entre lo reportado y la realidad del proceso
- Permitir seguimiento histórico de los riesgos

18.5 Mejora continua

Los resultados del monitoreo y reporte de riesgos deben ser utilizados para:

- Ajustar controles
- Fortalecer la gestión institucional
- Tomar decisiones estratégicas
- Actualizar el mapa de riesgos
- Identificar oportunidades de mejora
- Ajustar indicadores calves de riesgo

18.6 Contenido Mínimo de Informes de la Segunda Línea de Defensa.

- **Confirmación de la versión de la matriz objeto de seguimiento.**
- **Relación de los cambios efectuados** en las matrices de riesgos (incluye inactivaciones, nuevas formulaciones o ajustes).
- **Confirmación de la cuantificación** de los riesgos y controles (probabilidad, impacto, calificación y solidez del conjunto de controles).
- **Análisis de la gestión del riesgo durante el periodo**, comparando zonas de riesgo inherente vs. residual.
- **Seguimiento a riesgos materializados** y acciones vigentes para su tratamiento.
- **Confirmación de la oportunidad y cumplimiento** del cargue de soportes documentales que respalden la ejecución de los controles.
- **Observaciones** derivadas del análisis realizado.
- **Recomendaciones** a los líderes de procesos para mejorar la gestión de riesgos.
- **Conclusiones generales** del seguimiento efectuado.

18.7 Contenido Mínimo del Informe de la Oficina de Control Interno (Tercera Línea de Defensa)

- **Confirmación de la metodología** utilizada para el desarrollo del seguimiento.
- **Análisis de los resultados** obtenidos con base en el informe emitido por la segunda línea de defensa.
- **Evaluación de la estructura y clasificación** de los riesgos y controles (verificación de la coherencia técnica y metodológica).
- **Evaluación de la ejecución de los controles** (incluye cumplimiento de periodicidades, calidad de evidencias, pertinencia del diseño).
- **Seguimiento a la materialización de riesgos** (verificación del tratamiento, medidas adoptadas y continuidad de acciones).

Elaboró: Juan Carlos Cepeda Moncada – Contratista OAP
Revisó: Julián Pontón Silva – Jefe Oficina Asesora de Planeación

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co