ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SEGURIDAD,
CONVIVENCIA Y JUSTICIA

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE
SEGURIDAD, CONVIVENCIA
Y JUSTICIA
BOGOTÁ

1. OBJETIVO

Suministrar las pautas para la Administración del Riesgo de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ permitiendo identificar, analizar, controlar y mitigar los Riesgos por Proceso, Riesgos de Corrupción, Riesgos de Seguridad de la Información, Riesgos Estratégicos y Riesgos asociados a Lavado de Activos y Financiación del Terrorismo - LA/FT; que podrían afectar de manera negativa el logro de los objetivos estratégicos de la entidad, impidiendo la oferta adecuada, efectiva y optima de los servicios a la ciudadanía para los cuales fue concebida la SDSCJ. Propendiendo el desarrollo, implementación y mejora continua de la entidad en procesos globales, estrategia y planificación, gestión, procesos de presentación de informes, políticas, valores y cultura organizacional protegiendo el valor de la organización.

En este sentido, la SDSCJ procede con la adopción de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5" del Departamento Administrativo de la Función Pública – DAFP emitida en diciembre 30 de 2020, como lineamiento en la implementación de la administración de los Riesgos por Proceso, Riesgos de Corrupción y Riesgos de Seguridad de la Información.

A su vez, en atención a la "Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales" emitida por la Secretaria General de la Alcaldía Mayor de Bogotá D.C. la cual indica que las entidades privadas o públicas de índole nacional o territorial deben diseñar sistemas de administración de riesgos que les permita protegerse ante el riesgo asociado al lavado de activos (LA) y Financiación del Terrorismo (FT) y de esta forma dar cumplimiento a las obligaciones que se establecen en la normatividad vigente. Lo anterior, para evitar que sean utilizadas en el proceso de lavado de activos y financiación del terrorismo. Así entonces, la entidad se acoge a la recomendación como buena práctica para asociar y articular a su gestión de riesgos de riesgos de Corrupción, los criterios para la identificación, análisis y evaluación de riesgos asociados a LA/ FT.

La Gestión del Riesgo en la SDSCJ también se complementa con la Gestión de las Oportunidades, donde se identifican y desarrollan acciones que la entidad y los procesos deben aprovechar para aumentar el desempeño de la entidad articulado a lo definido en el Contexto estratégico de la entidad y los Riesgos Estratégicos asociados a los Objetivos Estratégicos. y

2. ALCANCE

Esta política busca puntualizar los lineamentos y criterios para la identificación, el análisis, el control, el seguimiento de los Riesgos Estratégicos, Riesgos por Proceso, de Corrupción, Riesgos de Seguridad de la Información, riesgos asociados a LA/ FT, y la gestión de Oportunidades de la SDSCJ contando con el análisis de factores internos y externos, estableciendo la metodología que se debe seguir para determinar la identificación, valoración y monitoreo y revisión de los eventos de riesgo, donde se contempla el diseño de los controles, además de la forma en que estos deben ser reportados y los periodos en los cuáles los líderes operativos deben realizar el cargue de las evidencias de ejecución de controles, hasta la elaboración de los informes de seguimiento de la segunda y tercera línea de defensa; propendiendo el desarrollo de estrategias que permitan el logro de objetivos y la toma de decisiones en todos los procesos que hacen parte de la SDSCJ.

Cabe destacar que los riesgos de seguridad de la Información se gestionarán en la entidad de acuerdo con los criterios diferenciales de la Política de Seguridad y Privacidad de la Información.

3. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ como líder y orientador de la seguridad de Distrito Capital, asume el compromiso de administrar los Riesgos por Proceso, Riesgos de Corrupción, Riesgos de Seguridad Información, Riesgos Estratégicos y Riesgos asociados a LAFT; que puedan afectar de manera negativa el alcance de los objetivos estratégicos y objetivos de procesos de la entidad; además de forjar una entidad más proactiva y detectiva que reactiva y correctiva, que trabaje en la reducción de los efectos no deseados y promoviendo la mejora continua, proyectando así, una organización basada en la acción preventiva automática, que controla todos los procesos de la entidad, brindando seguridad razonable y destinando los esfuerzos y recursos necesarios para administrar los riesgos que se puedan presentar en la SDSCJ.
Para lo anterior, es fundamental la determinación de la Capacidad del Riesgo, el nivel de Apetito del Riesgo y la Tolerancia del Riesgo lo cual se detalla en el desarrollo del presente documento.

La Gestión del Riesgo se complementa con la Gestión de las Oportunidades, donde se identifican las situaciones positivas que la entidad y los procesos deben aprovechar para aumentar el desempeño de la entidad.

4. NORMATIVIDAD

TIPO	DESCRIPCIÓN	EMITE/AUTOR
Artículo 73 de la Ley 1474 de 2011	Relacionado con la prevención de los riesgos de corrupción, - mapa de riesgos de corrupción.	Secretaría de Trasparencia de la Presidencia de la Republica
Ley Estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Congreso de la República
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	Congreso de la República
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.	Presidencia de la Republica
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 y se establece el MIPG	Presidencia de la Republica
Decreto 648 de 2017	Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública	Presidencia de la Republica
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 del 2015, decreto único reglamentario del sector de tecnologías de la información y las telecomunicaciones.	Presidencia de la Republica
Resolución 500 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.	Ministerio de las Tecnologías de la información y las comunicaciones
CONPES 3854 del 11 de abril de 2016, 3.2. Estrategia de gestión de riesgos de seguridad digita	El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad de la información, teniendo en cuenta el marco.	Consejo nacional de política económica y social república de Colombia Departamento Nacional de Planeación

5. 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.
Aceptar el Riesgo: decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
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.
ALA/CFT: Antilavado de Lavado de activos y Contra la Financiación del Terrorismo.
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).
Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
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).
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: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
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, fue creada mediante el Decreto 950 de 1995, modificado por los Decretos 754 de 1996, 2000 de 2003 y 3420 de 2004, de carácter permanente y adscrita el Ministerio de Justicia y del Derecho, y 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: Medida que permite reducir o mitigar un riesgo.
Control Correctivo: aquel que permite el restablecimiento de la actividad, después de detectarse un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.
Control Preventivo: aquel que actúa para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
Corrupción: es el abuso de poder o de confianza para el beneficio particular en detrimento del interés colectivo, en el que se incurre al ofrecer o solicitar, entregar o recibir bienes o dinero en especie, en servicios o beneficios a cambio de acciones, decisiones u omisiones (Transparencia Internacional, 2017).
Delito: es un comportamiento culpable y contrario a la Ley que conlleva una pena o sanción.
Delito fuente: comportamientos graves o peligrosos para la sociedad, listados de manera expresa por el legislador que generan el lavado de activos.
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 utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
Factores de Riesgo: Son las fuentes generadoras de riesgos.

Financiación del Terrorismo (FT): corresponde al conjunto de acciones que permiten la circulación de recursos que tienen como finalidad la realización de actividades terroristas o que pretenden el ocultamiento de activos provenientes de dichas actividades.
GAFI: Grupo de Acción Financiera Internacional para la Prevención del Lavado de Activos.
GAFISUD / GAFILAT: Organización Intergubernamental de base regional que agrupa 16 países de América del sur y Centroamérica para combatir el LA/FT.
Gestión del riesgo: un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
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: las consecuencias 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: propiedad de exactitud y completitud.
Lavado de Activos (LA): es el proceso mediante el cual organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas. En términos prácticos, es el proceso de hacer que dinero sucio parezca limpio, haciendo que las organizaciones criminales o delincuentes puedan hacer uso de dichos recursos y en algunos casos obtener ganancias sobre los mismos.
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 vinculantes o restrictivas: es la relación de personas naturales y jurídicas que pueden estar vinculadas con actividades de lavado de activos o financiación del terrorismo.
Mapa de riesgos: documento con la información resultante de la gestión del riesgo.
Mitigación: planificación y ejecución de medidas dirigidas a reducir o disminuir el riesgo identificado.
MSPI: Modelo de Seguridad y Privacidad de la Información

Monitoreo: comprobar, supervisar, observar críticamente, o registrar el proceso de una actividad, acción o sistema en forma sistemática, para identificar cambios.
Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general, la fórmula del Nivel del Riesgo 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.
Oficial de Cumplimiento: es la persona responsable del cumplimiento del sistema SARLAFT.
Operación inusual: es aquella operación que se sale de los parámetros normales o que por su cuantía y características no guarda relación con la actividad económica o comercial de cada uno de los grupos de interés.
Plan Anticorrupción y de Atención al Ciudadano (PAAC): Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
Personas Públicamente Expuestas (PEP): personas nacionales o extranjeras que por su perfil o por las funciones que desempeñan pueden exponer en mayor grado a la entidad al riesgo de LA/FT, tales como personas que por razón de su cargo manejan recursos públicos, detentan algún grado de poder público o gozan de reconocimiento público.
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: a cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.
Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Reporte de Operaciones sospechosa (ROS): corresponde a un hecho relacionado con la posible comisión de actividades relacionadas con los delitos de Lavado de Activos o Financiación del Terrorismo.
Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
Riesgo de Corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
Riesgo de Lavado de Activos y Financiación del Terrorismo – LA/FT: se define como la posibilidad de pérdida o daño que puede sufrir una Entidad por su propensión a ser utilizada directamente o a través de sus operaciones, como instrumento para el lavado de

activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

Riesgos de Seguridad de la Información: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.

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

Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

SARLAFT: Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo.

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: asiste y guía a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)

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: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
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.

6. TIPOS DE RIESGOS QUE SE VAN A CONTROLAR

Los tipos de riesgo a controlar en la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ y los cuales son mencionados a integridad en la presente Política de Administración de Riesgos, son los siguientes:

- Riesgos Estratégicos
- Riesgos por Proceso
- Riesgos de Corrupción junto a Riesgos asociados a LAFT
- Riesgos de Seguridad de la Información
- Oportunidades

Cada uno de los anteriores cuenta con su capítulo dentro del presente documento en el cual se especifica su gestión en la entidad.

7. 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 (que modifica al Decreto 1083 de 2015 por el cual se actualiza el MECI incluyéndolo de manera integral con el anterior Sistema Integrado de Gestión en el nuevo Modelo Integrado de Planeación y Gestión) y el Comité Institucional de Coordinación de Control Interno (reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017 para una adecuada gestión del riesgo) las entidades públicas deben estructurar lineamientos que orienten la toma de decisiones para el manejo y tratamiento de los riesgos identificados en los procesos, para lo cual la Secretaria Distrital de Seguridad, Convivencia y Justicia ha determinado los siguientes aspectos:

7.1 Roles y Responsabilidades

La Política de Administración del Riesgo es responsabilidad de todas las personas naturales y jurídicas que componen la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, así como, la implementación de una gestión adecuada de los Riesgos por Proceso, Riesgos de Corrupción, Riesgos de Seguridad de la Información, Riesgos Estratégicos, Riesgos asociados a LAFT y Oportunidades; la SDSCJ debe efectuar la formulación de la matriz respectiva con una participación integral y activa del líder del proceso y el líder operativo los cuales deben contar con el apoyo de los funcionarios y contratistas que hacen parte del proceso. Se deben seguir las etapas establecidas en la presente Política para cada caso, con el objetivo de identificar, analizar, dar tratamiento, seguimiento y evaluación a los riesgos que se estructuren. Todo con una visión completa del contexto interno y externo tanto de la entidad como del proceso, partiendo de las actividades propias que podrían desencadenar en un evento de riesgo, que deberán estar documentadas y controladas por el Sistema Integrado de Gestión.

7.2 Las líneas de defensa:

De acuerdo con el modelo de las líneas de defensa y lo definido en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Riesgos de Gestión, Corrupción y Seguridad de la Información” del Departamento Administrativo de la Función Pública, se define para la SDSCJ lo siguiente:

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.

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
En este comité se analiza la gestión del riesgo y se aplican las mejoras.

COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO
Corresponde al Comité de Control Interno aprobar la Política de administración del Riesgo y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo. A este comité debe subir el análisis de eventos y riesgos críticos

PRIMERA LÍNEA DE DEFENSA
Corresponde a los Líderes de Proceso y Líderes Operativos asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. A su vez, para todo tipo de riesgos debe garantizar el monitoreo y revisión periódica; en caso de ser necesario algún ajuste debe coordinar dicha gestión con la Segunda Línea defensa. Será su responsabilidad dar reporte de la materialización de los riesgos a la Segunda y Tercera línea de Defensa, así como, el cumplimiento del reporte y cargue de evidencias en los repositorios de información destinados para ello en

los tiempos estipulados por la Oficina Asesora de Planeación y lo mencionado en el presente documento.
Para efectos de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" el Gestor de Riesgos será desempeñado por el Líder Operativo de cada proceso.

SEGUNDA LÍNEA DE DEFENSA
Corresponde a la Oficina Asesora de Planeación ejecutar la consolidación de la gestión del riesgo estratégico, de gestión y corrupción, 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. Capacita, acompaña, genera recomendaciones con base a los lineamientos definidos.

La Dirección de Tecnologías y Sistemas de la Información consolida la información de la gestión del riesgo de seguridad de la información, 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. Capacita, acompaña, genera recomendaciones con base a los lineamientos definidos.

TERCERA LÍNEA DE DEFENSA
Le corresponde a la 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 entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

- Asesorar en coordinación con la Oficina Asesora de Planeación y la Oficina de Tecnología, a la primera línea de defensa en la análisis y valoración del riesgo, y en el diseño de los controles.
- Verificar la publicación del mapa 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.
- Recomendar mejoras a la política de administración del riesgo.
- Realizar evaluación a la gestión de Riesgos de la entidad.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN
Adicional a las líneas de defensa anteriormente mencionadas y 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 de los siguientes compromisos:

- 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.

7.3 Coordinación y Articulación

Los lineamientos de esta política deben ser aprobados y en caso de ser pertinente, modificados por medio del Comité Institucional de Coordinación de Control Interno, en cumplimiento a la resolución 215 de 2017.

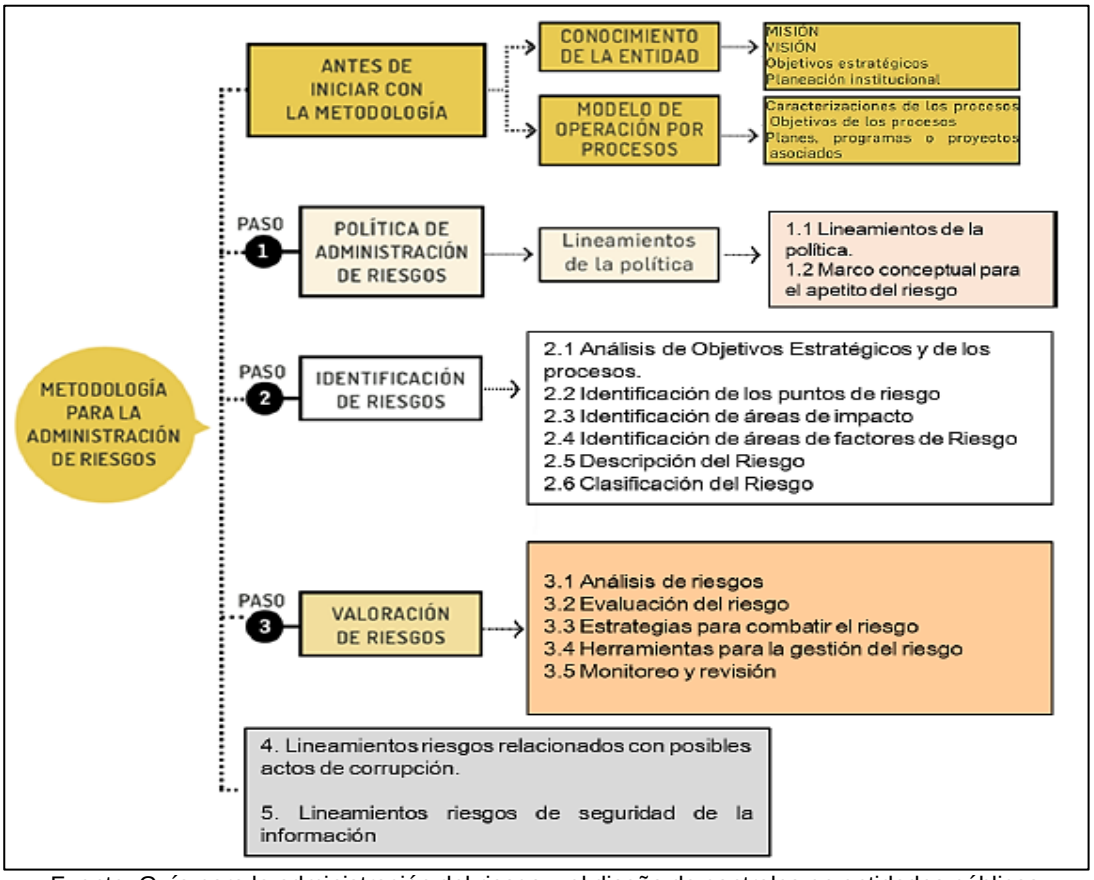
8. DERECHOS DE AUTOR

Todas las referencias a los documentos de la Política de Administración de Riesgos son derechos reservados por parte de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ.

En consecuencia, la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ goza de los derechos de autor establecidos en la ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos de la Política de Administración de Riesgos.

9. METODOLOGIA A IMPLEMENTAR

La Secretaria 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 complementa con la aplicación de la Metodología para la Administración de Riesgos ejecutando los tres (3) pasos básicos establecidos por la Guía del DAFP en caso de evidenciar alguno de los siguientes cambios: (1) en el contexto de la entidad, (2) relacionados con el “Conocimiento de la Entidad” o (3) del “Modelo de Operación por Procesos”. El ejercicio culmina con la oficialización y publicación de las Matrices por parte de la Oficina Asesora de Planeación con las cuales se inicia la gestión del año complementado por estrategias de comunicación a toda la entidad. A continuación, se puede observar la estructura completa con sus desarrollos básicos:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V.5.

10. IDENTIFICACIÓN Y GESTIÓN DEL RIESGO (RIESGOS POR PROCESO)

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, 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.

10.1 Etapa 1: Conocimiento de la actual Política de Administración de Riesgos y Divulgación de la Matriz de Riesgos por Procesos

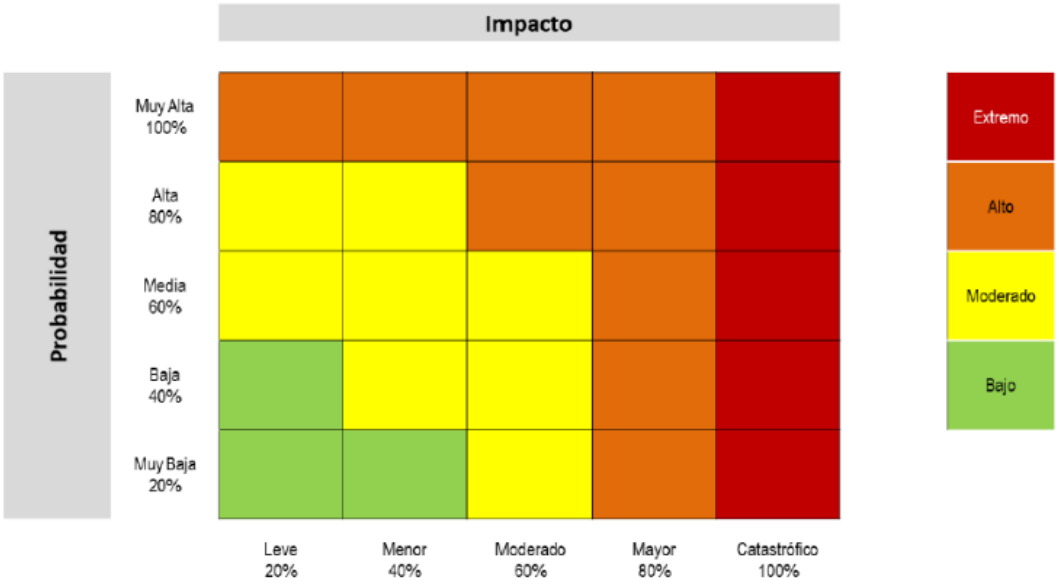
La presente Política debe ser de conocimiento general para los funcionarios y contratistas de la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, se debe tener en cuenta que en este documento se especifican los lineamientos técnicos con los cuales se ejecuta la gestión del riesgo en 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.

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

Intranet: Lineamientos y normatividad - Transparencia (planes - matriz de riesgo) - Matriz de riesgos por proceso
WEB: https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, Presupuesto e Informes - Plan de Acción - Matriz de riesgos por proceso

10.2 Etapa 2: Apetito, Tolerancia y Capacidad del Riesgo por Procesos

Para determinar el Apetito del Riesgo, Tolerancia del Riesgo y Capacidad del riesgo definidos en el Numeral 5 del presente documento, es necesario revisar en primer lugar en Nivel del Riesgo para los Riesgos por Procesos los cuales detallamos a continuación, gráficamente:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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** hasta Nivel de Riesgo **Extremo**.
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.

10.3 Etapa 3: Identificación del Riesgo

Para poder establecer la identificación del Riesgo existen varios aspectos que combinados permitirán un correcto análisis de los procesos los siguientes se recomienda el uso de al menos uno de ellos.

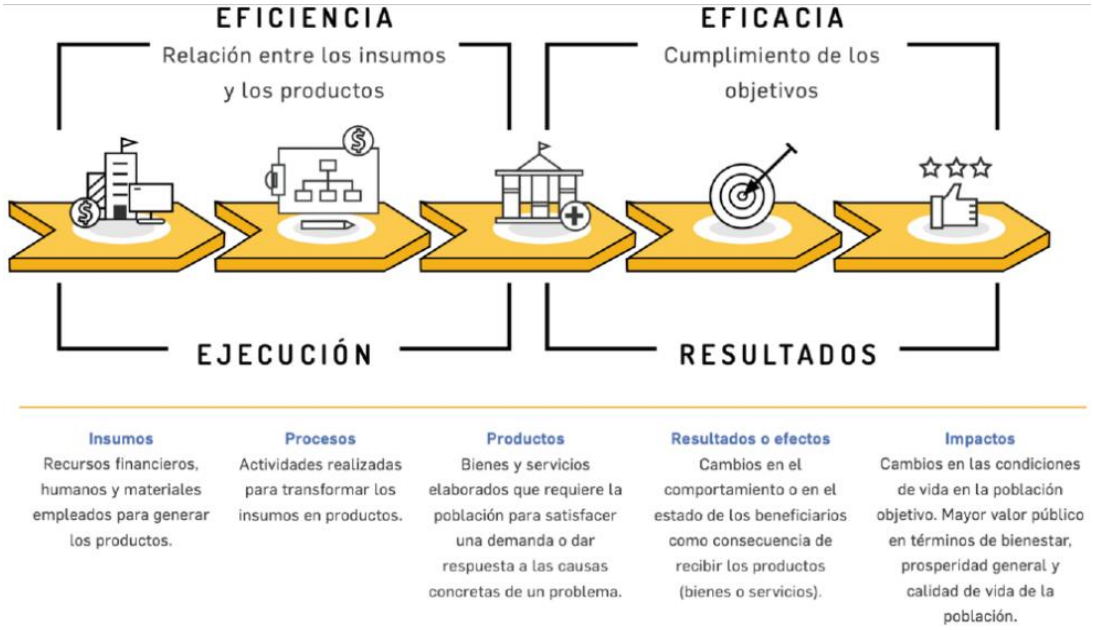
10.3.1 Análisis de Factores de Riesgo

En esta etapa se deben 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

10.3.2 Identificación y análisis de las actividades críticas del proceso

Dado que los objetivos estratégicos y de 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.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

10.3.3 Análisis de los Objetivos Estratégicos y de los Procesos

En una correcta construcción de objetivos por procesos se debe tener en cuenta la correlación que debe existir entre los objetivos estratégicos de la entidad y éstos, teniendo en cuenta el cumplimiento y cualquier situación que pueda representar su éxito o fracaso.

A su vez, los objetivos estratégicos deben estar alineados con la misión y visión de la entidad. Lo anterior permite una apropiada gestión de planeación que permitirá la identificación del riesgo en función de la afectación al logro y posible fracaso de los propósitos de la entidad.

Un objetivo debe contar con las siguientes características:

S ***Specific* (específico):** Lo importante es resolver cuestiones como: qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.

M ***Mensurable* (medible):** Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas (cuando aplique).

A ***Achievable* (alcanzable);** Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o cómo resultaría mejor.

R ***Relevant* (relevante):** Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación.

T ***Timely* (temporal):** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V.5.

A su vez, recomendamos la siguiente estructura para facilitar la construcción de objetivos de Indicadores de Gestión, Caracterizaciones de Proceso y procedimientos:

Fuente: Elaboración Propia

10.3.4 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 esto se recomienda se planteen 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.

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.

Se debe especificar que TODOS los procesos de la entidad deben tener al menos un riesgo por Proceso identificado, el cual debe estar debidamente estructurado en la Matriz de Riesgos por Proceso herramienta que ha sido definida por la entidad para la administración del Riesgo.

10.4 Etapa 4: 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-DS-573 **DOFA** (**Debilidades**, **Oportunidades**, **Fortalezas** y **Amenazas**), 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.

El ejercicio de la **DOFA** debe ser ejecutado adicionalmente en función de los objetivos estratégicos y los objetivos del proceso. Como mínimo, este ejercicio se debe realizar una vez al año y debe ajustarse las veces que sea necesario.

Fuente: Elaboración Propia

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.

DEBILIDADES	OPORTUNIDADES
• **Contexto interno** • **Contexto del proceso**	• **Contexto externo**
FORTALEZAS	**AMENAZAS**
• **Contexto interno** • **Contexto del proceso**	• **Contexto externo**

Fuente: Elaboración Propia

Identificado el contexto o factor, se debe clasificar el riesgo en las siguientes categorías teniendo en cuenta la interrelación y el origen establecido para el Factor de acuerdo con la DOFA realizada:

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.

Fuente: Elaboración Propia

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	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal

Factor	Definición	Descripción
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurtos activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Elaboración Propia

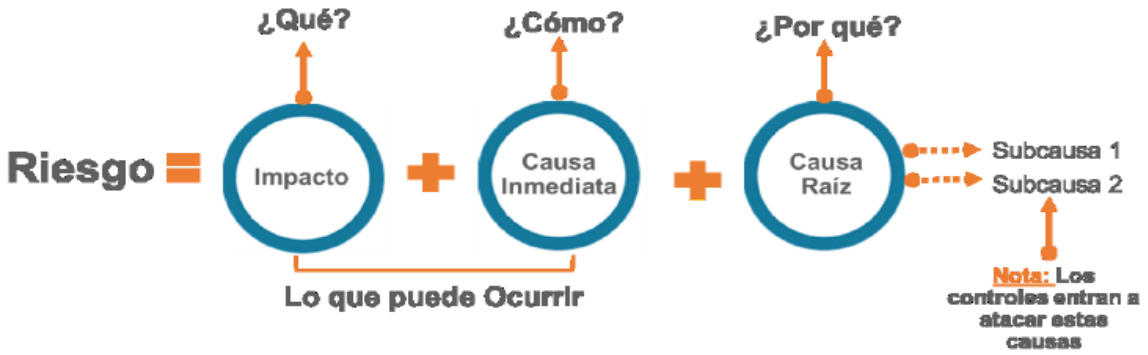
Identificado lo anterior, se debe establecer la Causa Raíz y la Causa Inmediata de acuerdo con lo siguiente:

- **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.

10.5 Etapa 5: Estructuración del riesgo

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 (o presupuestal) y reputacional.

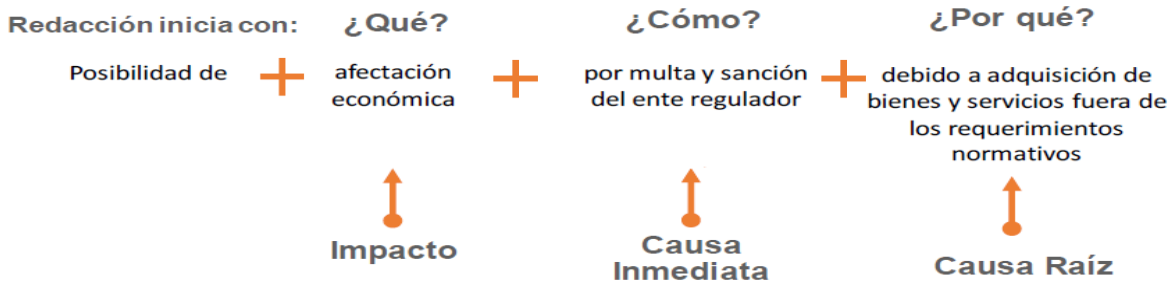
Dado lo anterior, la siguiente será la estructura del Riesgo partiendo del Impacto y lo mencionado en la Etapa 4:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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.

10.6 Etapa 6: Valoración del riesgo por proceso

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 y ajustada con base a la realidad de la entidad:

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%

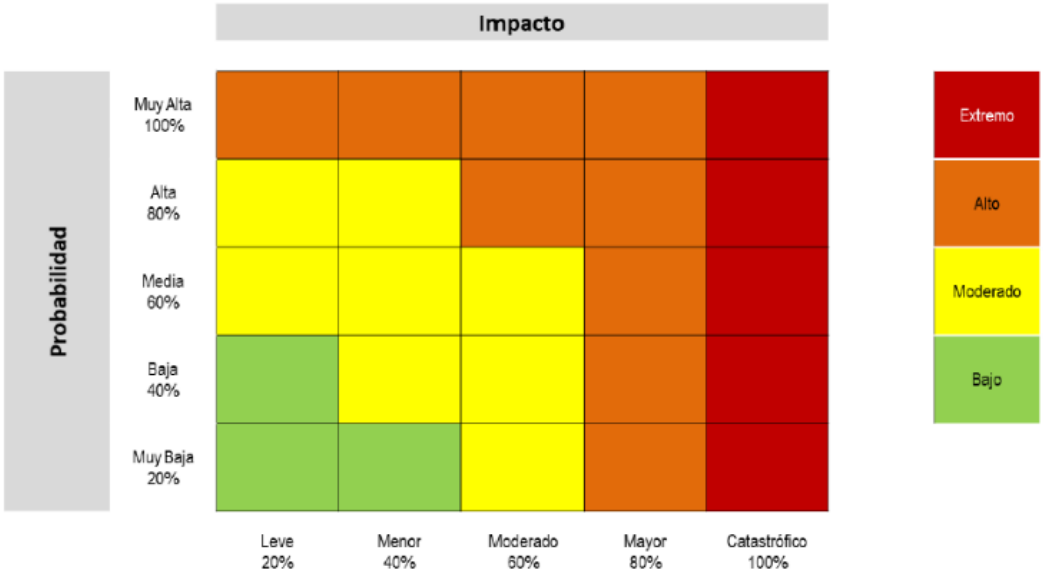
Fuente: Elaboración Propia

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%
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%

Fuente: Elaboración Propia

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 (P vs I) en el siguiente mapa de calor.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

El mapa 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 de la siguiente forma:

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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)*.

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.

10.7 Etapa 7: 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.

10.7.1 Estructura de Controles

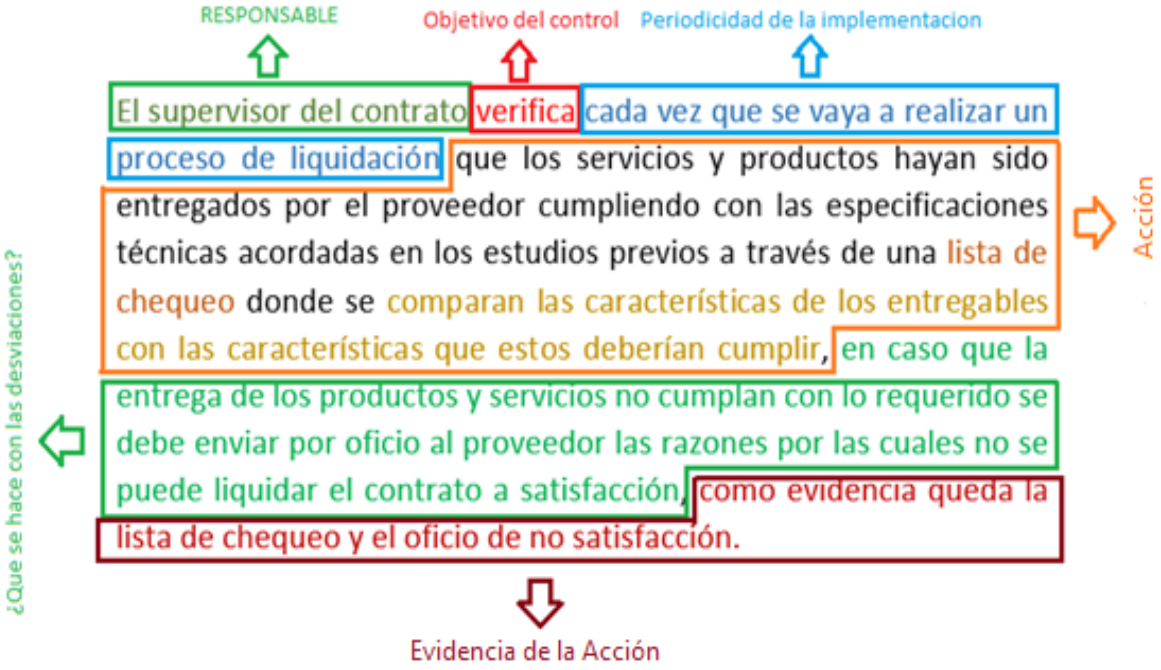
Para que un control este adecuadamente diseñado y que su implementación sea efectiva a la hora de mitigar un riesgo éste debe cumplir con los siguientes lineamientos:

- Debe tener un **responsable de su ejecución**, identificar el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identifica el sistema que realiza la actividad. (Evitar colocar áreas generales o nombres propios), por ejemplo: responsable de inventarios.
- En la descripción del control se debe especificar como se ejecuta **la Acción** del control.
- 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 debe incluir **cuál es el Objetivo** 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.

Notas:

- *Se solicitará el Cargue Trimestral de evidencias para todos los controles, para aquellos casos en los cuales la periodicidad de ejecución de la actividad sea superior a la fecha de cargue de evidencias se deberá adjuntar un soporte que permita verificar los avances o proyección de ejecución de la actividad control.*
- *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.*
- *Se recomendará el uso de Matrices gerenciales para los casos en los cuales se presente manejo de información reservada o clasificada, con las cuales se logre evidenciar la ejecución de las actividades control.*
- *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.*

La siguiente es la estructura para los controles recomendada.



Fuente: Elaboración Propia

10.7.2 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.

La Oficina Asesora de Planeación propenderá la estructura de controles de los tres tipos para todos los procesos.

Otra tipología existente corresponde al cómo se ejecuta el control **(implementación)**, para ello se tienen las siguientes:

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

10.8 Etapa 8: Calificación del control

Una vez se haya estructurado el control se debe evaluar el atributo teniendo en cuenta lo mencionado en el **Numeral 10.7 Etapa 7**. 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.

A continuación, se presentan los criterios para la aplicación de los atributos para el análisis y valoración de los controles propuestos, con ello se busca obtener una calificación, en cumplimiento de las características mencionadas en el numeral antes mencionado, 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	-
		Objetivo	Cuenta con un Objetivo	-
		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	-

Fuente: Elaboración Propia

Como se puede evidenciar, los Atributos Informativos de Cumplimiento no tienen peso porcentual; sin embargo, son obligatorios, motivo por el cual todo control debe contener dichas características, caso contrario no podrá ser contemplado para su oficialización y vinculación a la Matriz de Riesgos por Procesos. Se debe resaltar que no solo basta con que el control esté debidamente diseñado, sino también se tiene que velar por su implementación y ejecución.

Inicialmente la determinación de ejecución del control es una confirmación por parte del responsable del proceso, y posteriormente se debe confirmar con el cargue de las evidencias de las actividades del control en los periodos de corte establecidos dentro de la presente Política, posterior el profesional de la Administración de Riesgos de la Oficina Asesora de Planeación elabora un Informe de Seguimiento al vencimiento de cada periodo, que a su vez, será evaluado por Control Interno o Auditoría Interna.

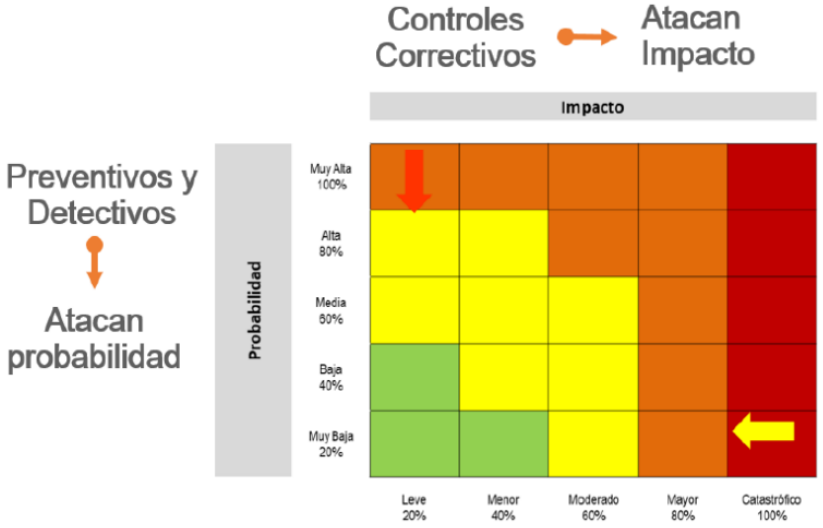
Continuando con los criterios de Evaluación del Control, se establecerá la calificación de la ejecución del control con base en la siguiente tabla:

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.

Fuente: Elaboración Propia

10.9 Etapa 9: 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.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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

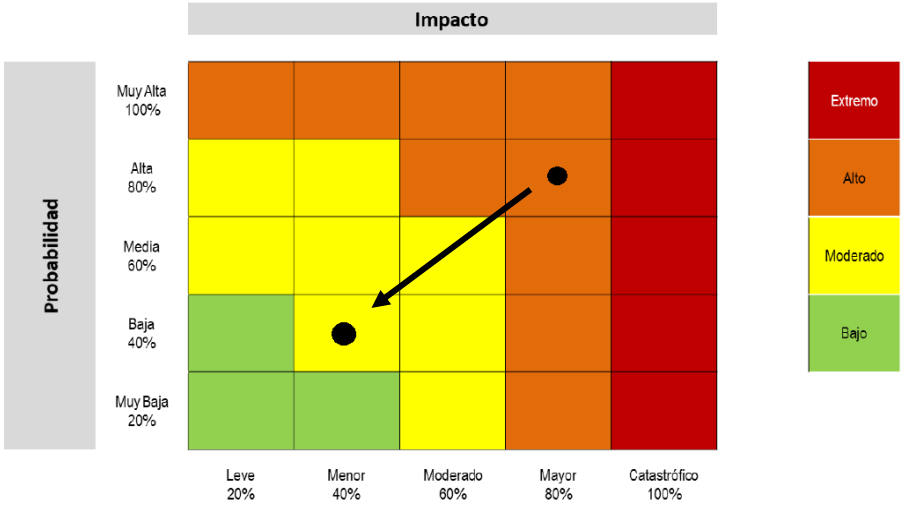
IMPACTO

La formulación es la siguiente:

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

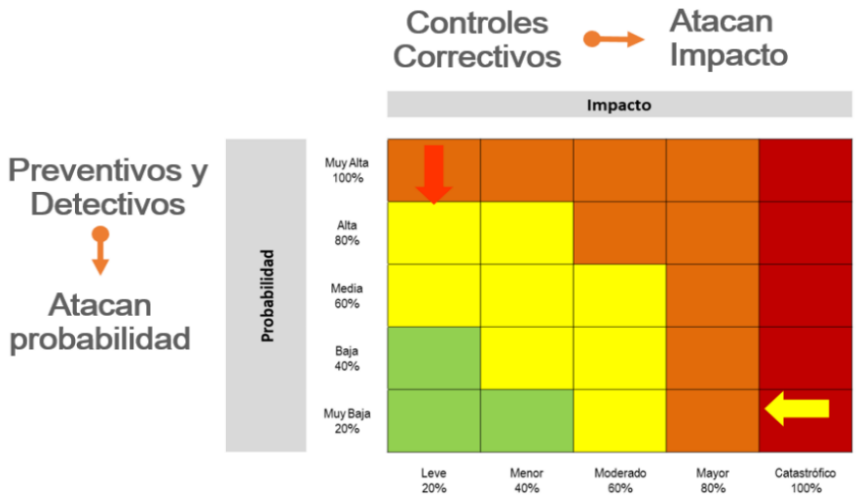
$$IR_n = II_1 - (II_1 * VCC)$$

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. El desplazamiento en el Mapa de Calor debe ser similar a la siguiente, siempre propendiendo una disminución en la Zona de Riesgo contando con las tres tipologías Preventivo-Detectivo-Correctivo.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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 Eficiciencia del control.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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 tanto 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 el numeral **12.4** del presente documento.

10.10 Etapa 10: 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 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.

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

11. IDENTIFICACIÓN Y GESTIÓN DEL RIESGO (RIESGOS DE CORRUPCIÓN)

La gestión de los Riesgos de Corrupción difiere en varios aspectos sobre la ejecución de actividades con relación a los Riesgos por Proceso, por esta razón el DAFP hace una leve separación en el enfoque con el cual se administran estas dos tipologías de riesgos.

A continuación, se brindan los parámetros para administrar correctamente los Riesgos de Corrupción, reiterando que se debe partir de los lineamientos básicos precisando y analizando el contexto general de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, enmarcando principalmente la planeación institucional, el modelo de operación, la cadena de valor, el mapa de procesos, los objetivos estratégicos, la caracterización de los procesos, la misión y la visión para lograr establecer su complejidad y de esta forma conocer y entender la entidad y su entorno, lo que determina el análisis de riesgos y la aplicación de la metodología en general confirmando que se hace necesaria una participación integral entre el líder del proceso, el líder operativo y los funcionarios del mismo propendiendo que la identificación, el análisis, la gestión, el tratamiento y el seguimiento de los riesgos, se lleve a cabo con una visión integral de todas las actividades propias de la SDSCJ que podrían desencadenar en un evento de riesgo.

Por otro lado, en atención a la “Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales” de la Secretaria General de la Alcaldía Mayor de Bogotá D.C. que indica que las entidades privadas o públicas de índole nacional o territorial deben diseñar sistemas de administración de riesgos que les permita protegerse ante el 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. Lo anterior, para evitar que sean utilizadas en el proceso de lavado de activos y financiación del terrorismo. Así entonces, la entidad se acoge a la recomendación como buena práctica para asociar y articular a su gestión de riesgos de riesgos de corrupción, los criterios para la identificación, análisis y evaluación de riesgos asociados a LA/ FT.

Se requiere del compromiso a todo nivel iniciando por la autoridad de la organización, el equipo directivo y todos los funcionarios, para el cumplimiento efectivo y eficiente del sistema SARLAFT.

Para aquellas etapas que tengan el mismo tratamiento que los Riesgos por Procesos (numeral 10), se indicara el numeral correspondiente donde se encontrara la metodología a seguir, lo anterior con el fin de evitar reiterar información dentro del presente documento.

A continuación, las etapas se deben seguir para garantizar la perfecta administración del Riesgo de Corrupción:

11.1 Etapa 1: Conocimiento de la actual Política de Administración de Riesgos y los riesgos de corrupción

La primera etapa de la gestión de los Riesgos de Corrupción sigue los mismos lineamientos expuestos en el numeral **10.1** a diferencia de la ubicación de la matriz que se expresa a continuación.

La siguiente información se puede detallar, verificar y validar en la Matriz General de Riesgos de Corrupción que es publicada en Intranet y en la página WEB de la SDSCJ siguiendo las siguientes rutas:

- **Intranet**. Lineamientos y normatividad - Transparencia (planes - matriz de riesgo) - Plan Anticorrupción y de Atención al Ciudadano - Mapa de Riesgos de Corrupción
- **WEB**. https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, Presupuesto e Informes - Plan de acción - Plan Anticorrupción y de Atención al Ciudadano - Mapa de Riesgos de Corrupción

11.2 Etapa 2: Identificación del Riesgo

La segunda etapa en la gestión de Riesgos de Corrupción sigue los mismos lineamientos expuestos en el numeral **10.3.**

Adicionalmente, se presenta el flujo de Lavado de Activos y Financiación del Terrorismo donde el lavador puede acudir a la entidad para transformar el dinero producto de la comisión de actividades ilícitas utilizando los canales que ofrecen las instituciones y disfrutar de las ganancias ilícitas, como se muestra en la ilustración.

Fuente: Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales

Lo anterior se puede presentar en alguno de los siguientes escenarios:

Escenario 1. Es posible que la entidad pueda verse afectada por este tipo de riesgo debido a que su actividad se encuentra enfocada al ofrecimiento de productos, bienes o servicios

y como contraprestación reciben directamente recursos que provienen de clientes y/o usuarios que pueden tener cierto grado de exposición al riesgo de LA/FT.
Escenario 2. Si bien la entidad no genera ingresos derivados de su función social, puede recibir recursos de entidades privadas, donaciones o inversión externa que puedan estar destinadas a la financiación de proyectos que requieren procesos de contratación, los cuales por su número y cuantía son significativos y pueden presentar vulnerabilidad al riesgo de LA/FT.

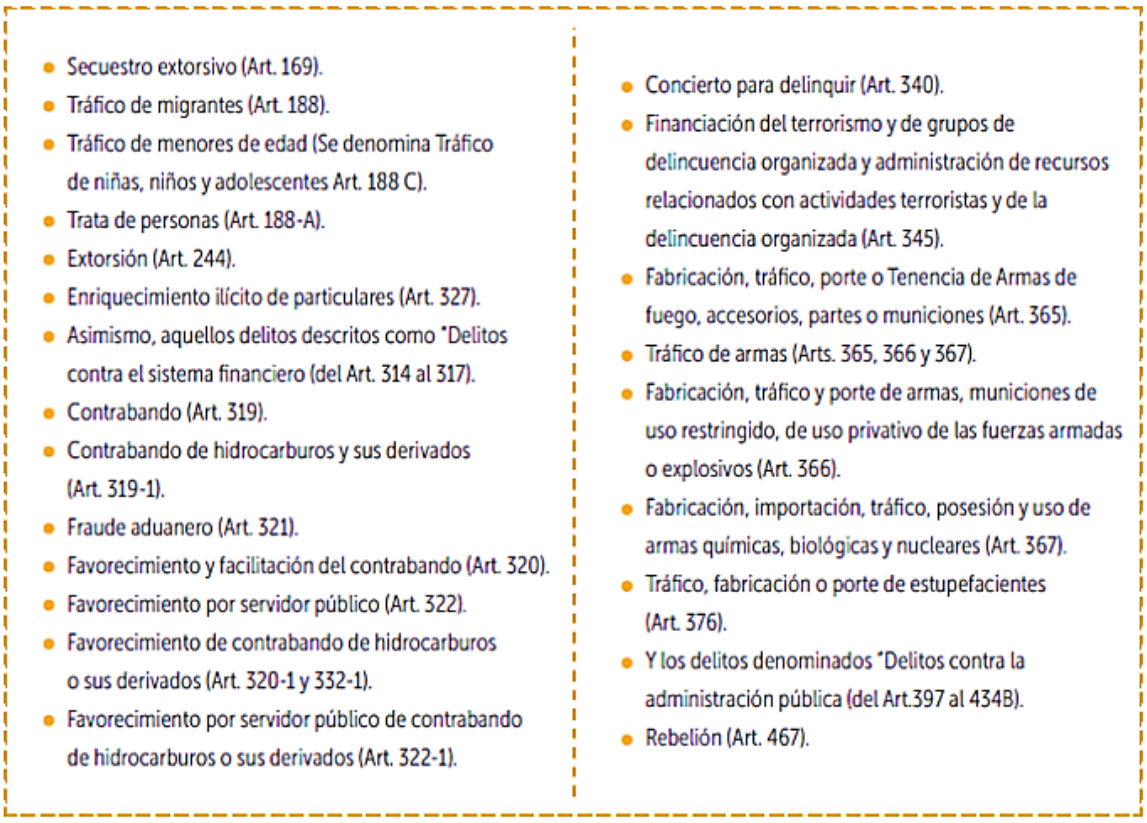
Estos hechos, actividades o situaciones se ven relacionados con los factores internos o externos generadores del riesgo de LA/FT, que pueden ser los clientes, usuarios, proveedores, empleados, productos, canales de distribución y zonas o jurisdicciones de alto riesgo, que afectan la multiplicidad de acciones que realizan las entidades. A continuación, se detallan a manera de ejemplo algunas características generales del LA/FT que facilitan su identificación:

a) El agente generador de riesgo (lavado de activos), asume perfiles que no corresponden a su realidad, aparentando, simulando o engañando a través de cualidades, negocios o posición económica que no posee.
b) Las organizaciones que se dedican al lavado de activos utilizan a personas de escasos recursos que tiene perfil social, económico o cultural bajo o modesto para enmascarar sus operaciones.

Señales de alerta identificadas:

- Información insuficiente o falsa entregada por el cliente (agente generador del riesgo).
- Empleados con un estilo de vida que no corresponde con el monto de su salario.
- Operaciones que por su monto y número no coinciden con la capacidad económica y perfil del cliente.
- Proveedores que ofrecen productos a menor precio de los existen en el mercado.
- Inconsistencias en los datos de la empresa, representante legal y/o socios en el proceso de verificación por parte de la entidad.

Generalmente la actividad ilegal que se asocia con en LA/FT es el narcotráfico. Sin embargo, no es la única asociada por ello a continuación podremos visualizar algunas actuaciones adicionales que pueden verse relacionadas:



- Secuestro extorsivo (Art. 169).
- Tráfico de migrantes (Art. 188).
- Tráfico de menores de edad (Se denomina Tráfico de niñas, niños y adolescentes Art. 188 C).
- Trata de personas (Art. 188-A).
- Extorsión (Art. 244).
- Enriquecimiento ilícito de particulares (Art. 327).
- Asimismo, aquellos delitos descritos como "Delitos contra el sistema financiero (del Art. 314 al 317).
- Contrabando (Art. 319).
- Contrabando de hidrocarburos y sus derivados (Art. 319-1).
- Fraude aduanero (Art. 321).
- Favorecimiento y facilitación del contrabando (Art. 320).
- Favorecimiento por servidor público (Art. 322).
- Favorecimiento de contrabando de hidrocarburos o sus derivados (Art. 320-1 y 332-1).
- Favorecimiento por servidor público de contrabando de hidrocarburos o sus derivados (Art. 322-1).
- Concierto para delinquir (Art. 340).
- Financiación del terrorismo y de grupos de delincuencia organizada y administración de recursos relacionados con actividades terroristas y de la delincuencia organizada (Art. 345).
- Fabricación, tráfico, porte o Tenencia de Armas de fuego, accesorios, partes o municiones (Art. 365).
- Tráfico de armas (Arts. 365, 366 y 367).
- Fabricación, tráfico y porte de armas, municiones de uso restringido, de uso privativo de las fuerzas armadas o explosivos (Art. 366).
- Fabricación, importación, tráfico, posesión y uso de armas químicas, biológicas y nucleares (Art. 367).
- Tráfico, fabricación o porte de estupefacientes (Art. 376).
- Y los delitos denominados "Delitos contra la administración pública (del Art.397 al 434B).
- Rebelión (Art. 467).

Fuente: Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales

Para afrontar lo anteriormente descrito se desarrolla el SARLAFT (Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo), sistema que está compuesto por varios pasos y elementos que contribuyen a promover la cultura de gestión del riesgo en las entidades, con el fin de prevenir que puedan utilizarse en las etapas del LA/FT para dar apariencia de legalidad a recursos ilícitos originados de actividades delictivas. Entre las etapas encontramos según el modelo GAFI13 las siguientes:

- **Colocación:** consiste en la recepción física de bienes de cualquier naturaleza o de dinero, en desarrollo y como consecuencia de actividades ilícitas que pretenden ponerse en el sistema económico.
- **Transformación:** consiste en la introducción de los fondos (dinero físico) o bienes, en la economía legal, seguida de sucesivas operaciones (nacionales o internacionales), para ocultar, invertir, o para mezclarlos con dinero de origen legal, con el fin de disimular su origen.
- **Integración:** en este paso, el dinero lavado regresa a la economía disfrazado ahora como "dinero legítimo".

11.3 Etapa 3: Identificación del riesgo de corrupción

En esta etapa el Líder del Proceso debe analizar con el Líder Operativo, en apoyo con la asesoría del Profesional encargado para la Gestión del Riesgo de la OAP, que eventos de riesgo con características de Corrupción se podrían presentar en la ejecución de las actividades críticas del proceso detalladas en la ejecución del numeral **10.3**.

Para evitar confusiones sobre la naturaleza de un Riesgo por Proceso y un Riesgo de Corrupción el DAFP brinda la siguiente definición de un riesgo de corrupción:

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

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

Dado lo anterior, para que un riesgo sea clasificado como un Riesgo de Corrupción debe cumplir con la siguiente estructura:

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

Se debe aclarar que, a partir de la anterior versión del presente documento, todos los procesos de la entidad deben contar al menos con un Riesgo de Corrupción identificado, este a su vez debe estar representado en la Matriz de Riesgos de Corrupción de la entidad. Para aquellos procesos que por la naturaleza y ejecución de sus actividades no representen un ambiente probable para que este tipo de riesgos se materialicen deberá ser determinado en las mesas de trabajo dejando la respectiva evidencia de lo identificado.

Adicionalmente, se deben resolver los siguientes cuestionarios para identificar el grado de vulnerabilidad de la entidad y de los procesos frente al SARLAFT:

Cuestionario sobre el Riesgo Operativo			
Preguntas	**SI**	**NO**	**NA**
1. ¿La entidad recibe recursos de entidades privadas?			
2. ¿La entidad recibe donaciones?			
3. ¿La entidad genera recursos propios derivados de bienes, productos o servicios ofrecidos?			
4. ¿La entidad realiza operaciones internacionales en divisas?			
5. ¿La entidad realiza operaciones en efectivo en el desarrollo de sus actividades?			
6. ¿Los clientes de la entidad corresponden al público en general ?			
7. ¿Los clientes objetivo de la entidad son personas naturales entre las que se encuentran las personas expuestas políticamente (PEP's)?			
8. ¿ La entidad cuenta con clientes que son personas jurídicas constituidas en el país?			
9. ¿En algún momento un proveedor de la entidad se ha negado a suministrar la información que se le solicita?			
10. ¿En la entidad existe una alta rotación de sus proveedores nacionales y extranjeros o los están cambiando con frecuencia?			
11. ¿La entidad emplea terceros para llevar a cabo alguna de las funciones en el cumplimiento de sus objetivos?			

Nivel de riesgo operativo	*Si el número de respuestas positivas se encuentra entre*
BAJO	1 y 3
MODERADO	4 y 5
MEDIO	6 y 7
ALTO	8 y 9
CRÍTICO	10 y 11

Exposición

Fuente: Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales

El resultado obtenido permitirá determinar el grado de exposición relacionado con los riesgos operativos, y servirán de insumo para la estructuración de Riesgos de Corrupción con base a las respuestas recibidas.

La siguiente encuesta nos permitirá establecer el estado actual frente a los Riesgos que se pueden presentar respecto al SARLAFT y que deben incluirse en la Matriz de Riesgos de Corrupción.

Cuestionario sobre los controles del riesgo de LA/FT

Preguntas	SI	NO	NA
1. ¿En la entidad existe una política clara sobre las donaciones?			
2. ¿Cuenta su entidad con un área encargada de administrar las bases de datos?			
3. ¿La entidad cuenta con mecanismos para conocer el cliente?			
4. ¿La entidad cuenta con mecanismos para conocer los proveedores?			
5. ¿La entidad cuenta con mecanismos para identificar el usuario?			
6. ¿La entidad en el desarrollo de su actividad ha identificado situaciones relacionadas de LA/FT?			
7. ¿Ha identificado si la entidad puede estar expuesta al riesgo de contagio de LA/FT en el desarrollo de sus funciones?			
8. ¿La entidad cuenta con manuales, políticas y procedimientos para abordar el riesgo de LA/FT?			
9. ¿En la entidad se han realizado jornadas de capacitación sobre los sistemas de administración de riesgo de LA/FT?			
10. ¿La entidad cuenta con un mapa de riesgo en el que se identifiquen los riesgos de LA/FT?			
11. ¿La entidad cuenta con sistemas de monitoreo para sus clientes y/o usuarios y sus operaciones ?			
12. ¿La entidad se encuentra sujeta a regulación sobre la prevención y control del riesgo de LA/FT?			
13. ¿La entidad cuenta con bases de datos con información de sus clientes y/o usuarios?			
14. ¿La entidad cuenta con bases de datos con información de sus proveedores?			
15. ¿La entidad cuenta con el mapeo de zonas de alto riesgo para sus operaciones?			
16. ¿Dentro de la entidad existen áreas que por sus funciones pueden ser vulnerables al LA/FT?			
17. ¿La entidad conoce las señales de alerta de LA/FT del sector al cual pertenece?			
18. ¿La entidad ha realizado reportes a la UIAF?			
19. ¿La Entidad destina recursos humanos, tecnológicos y financieros específicos para garantizar la implementación efectiva del programa LA/FT?			

Preguntas	SI	NO	NA
20. ¿Tiene la entidad políticas para comunicar nuevas leyes LA/FT o cambios a las existentes políticas o prácticas relacionadas a los empleados u otras Entidades?			
21. ¿La Entidad cuenta con un registro de sus sesiones de entrenamiento, incluyendo registros de asistencia y los materiales relevantes de entrenamiento sobre LA/FT?			
22. ¿Proporciona la entidad entrenamiento LA/FT a empleados que incluye identificación de señales de alerta que deben ser informadas internamente, ejemplos de diferentes formas de lavado de dinero que implican los productos y servicios de la Entidad, políticas internas para evitar el lavado de dinero, entre otros temas?			
23 ¿Tiene la entidad un programa de monitoreo para la detección de actividades sospechosas o inusuales de LA/FT?			
24. ¿Tiene la entidad procedimientos para identificar transacciones estructuradas efectuadas con el objeto de evitar los requisitos de reportar sobre grandes cantidades de efectivo?			
25. ¿Tiene la entidad políticas para asegurar razonablemente que sólo opera con bancos y entidades financieras debidamente autorizadas?			
26. ¿Existe un procedimiento para revisar y cuando sea apropiado, actualizar la información y documentación de sus clientes y/o usuarios, principalmente los que representan alto riesgo?			
27. ¿La entidad cuenta con políticas escritas que cubran las relaciones con personas políticamente expuestas – PEP's, su familia, asociados y estrechos colaboradores de acuerdo a las mejores prácticas?			
28. ¿En la entidad existe un procedimiento para la verificación de los nombres de sus clientes contra listas gubernamentales de narcotraficantes o terroristas, listas de riesgo privadas o listas de riesgo públicamente disponibles?			
29. ¿Requiere la entidad que sus políticas y prácticas de LA/FT sean aplicadas a todas las oficinas y dependencias?			
30. ¿Su entidad tiene auditoría interna y/o externa que monitoree y/o audite el sistema de prevención del LA/FT?			
31. ¿La entidad cuenta con manuales de gobierno corporativo (buen gobierno), ética u otros?			
32. ¿La entidad cuenta con Identificación de riesgos de LA/FT a los que está expuesta la compañía?			
33. ¿La entidad efectúa registro de validación de clientes?			
34. ¿La entidad a identificado señales de alerta de LA/FT propias?			
35. ¿La junta o consejo directivo cuenta con un reglamento escrito de sus funciones adicional al de los estatutos?			
36. ¿El área de auditoría y/o control interno conoce las responsabilidades y consecuencias frente al LA/FT?			
37. ¿En la entidad existe un procedimiento de solicitud, verificación y validación de la información proporcionada por clientes o empleados al momento de vincularse a la entidad?			

Cuestionario sobre los controles del riesgo de LA/FT			
Preguntas	**SI**	**NO**	**NA**
38. ¿La entidad realiza ECTH (estudio de confiabilidad del talento humano)?			
39. ¿Considera usted que la entidad cuenta los sistemas informáticos y aplicativos que le permitan identificar riesgos y le permitan prevenir el LA/FT?			
40. ¿Sus sistemas informáticos y/o aplicativos, tienen la capacidad de detectar comportamientos inusuales y/o atípicos de sus clientes y proveedores?			
41. ¿Su entidad cuenta con medidas de contingencia en caso de que falle el sistema informático?			
42. ¿Su entidad cuenta con las medidas informáticas necesarias para proteger su información?			
43. ¿La entidad tiene identificadas las zonas o jurisdicciones de alto riesgo?			
44. ¿La entidad ha identificado los factores internos y externos generadores de riesgo de LA/FT?			

Fuente: Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales

Dadas las respuestas al cuestionario, se puede tener una autoevaluación sobre el avance en la aplicación de herramientas antilavado de activos y contra la financiación del terrorismo, y la vulnerabilidad de la entidad frente a este tipo de riesgo.

Nivel de riesgo	*Si el número de las respuestas positivas se encuentran entre* — *Control del riesgo de LA/FT*		*Se debe tomar medidas sobre el manejo del riesgo de LA/FT*
BAJO	36 y 45	Vulnerabilidad	**Continuamente** Monitorear constantemente los riesgos.
MODERADO	27 y 35		**Integralmente** Complementar los controles
MEDIO	18 y 26		**Oportunamente** Establecer controles que reduzcan el riesgo
ALTO	9 y 17		**Prioritariamente** Adoptar un sistema de administracion de riesgos
CRÍTICO	1 y 8		**Urgentemente** Implementar un sistema de administración de riesgos

Fuente: Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales

Las anteriores encuestas deben ser resueltas por los Líderes de Procesos o Líderes Operativos como mínimo una vez al Año para garantizar el desarrollo periódico que permita obtener los diferentes cambios que se presenten en la entidad.

11.4 Etapa 4: Identificación y análisis de las causas

La quinta etapa de la gestión de Riesgos de Corrupción sigue los mismos lineamientos que dicta el numeral **10.4.**

11.5 Etapa 5: Estructuración del riesgo de corrupción

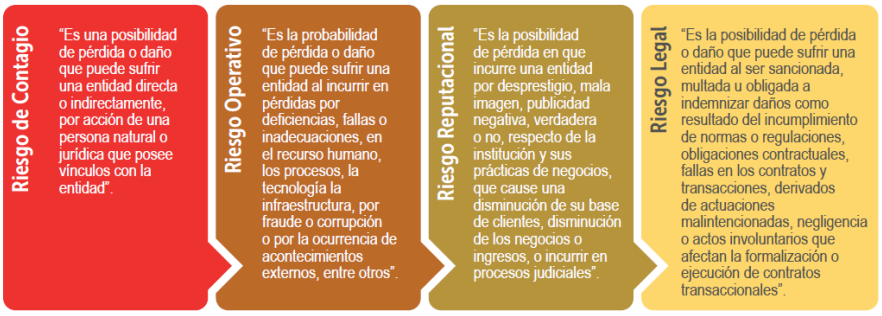
Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se debe utilizar la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de efectuada en el numeral **11.3** de la siguiente forma:

Matriz definición del Riesgo de Corrupción				
Descripción del riesgo	Acción u omisión	Uso del Poder	Desviar la gestión de lo público	Beneficio privado

Fuente: Elaboración Propia

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 Corrupción sino a un Riesgo de Procesos.

Adicionalmente, se consulta a todos los procesos sobre la posibilidad de presencia de alguno de los siguientes Riesgos los cuales se incluirán en la Matriz de Riesgos de Corrupción en caso de evidenciarse:



Fuente: Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales

11.6 Etapa 6: Valoración del riesgo de corrupción

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 por medio de la siguiente tabla:

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

Para los Riesgos de Corrupción el impacto se determina diligenciando el formulario “CALIFICACIÓN DE IMPACTO”, que busca decretar cuáles serían las consecuencias de dicha materialización dada la cantidad de respuestas afirmativas al cuestionario, ubicando dicho impacto en los rangos MODERADO, MAYOR y CATASTRÓFICO.

Responder afirmativamente de UNO a CINCO pregunta(s) genera un impacto **Moderado.** Responder afirmativamente de SEIS a ONCE preguntas genera un impacto **Mayor.** Responder afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto **Catastrófico.**	
MODERADO	Genera medianas consecuencias sobre la entidad
MAYOR	Genera altas consecuencias sobre la entidad.
CATASTROFICO	Genera consecuencias desastrosas para la entidad

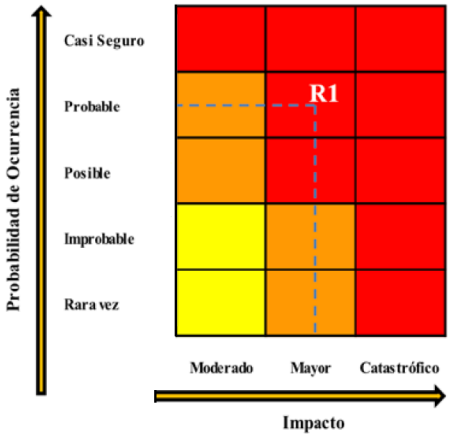
Nro	PREGUNTA: Si el riesgo de corrupción se materializa podría...	Respuesta	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la Entidad?	X	
4	¿Afectar el cumplimiento de la misión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

Nivel de Impacto **MAYOR**

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

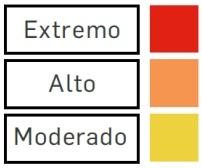
Como se puede evidenciar para los Riesgos de Corrupción solo hacemos uso de tres niveles de impacto (moderado, mayor y catastrófico) que son resultado de la cantidad de afirmaciones obtenidas en las preguntas del cuestionario, proyecta la posibilidad de materialización del riesgo afectando o generando alguna de las situaciones descritas.

A continuación, representamos el mapa de calor en cual se ubica el riesgo inherente de un evento de corrupción luego de su identificación:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

El mapa de calor cuenta con cinco niveles de ubicación para la probabilidad y tres niveles para el impacto, los cuales se ubican en tres zonas determinadas de la siguiente forma:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

En el caso de los Riesgos de Corrupción 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 Corrupción, 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.

11.7 Etapa 7: Tratamiento del riesgo de corrupción

Teniendo en cuenta que los niveles de impacto establecidos para los riesgos de corrupción 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 diseñar 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.

11.7.1 Tipos de controles

Se tienen dos tipos de controles:

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:

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.

La Oficina Asesora de Planeación propenderá la estructura de Controles que sean preventivos y detectivos para todos los procesos.

11.7.2 Características de un control adecuadamente estructurado

Para que un control este adecuadamente diseñado y que su implementación sea efectiva a la hora de mitigar un riesgo éste debe cumplir con los siguientes lineamientos:

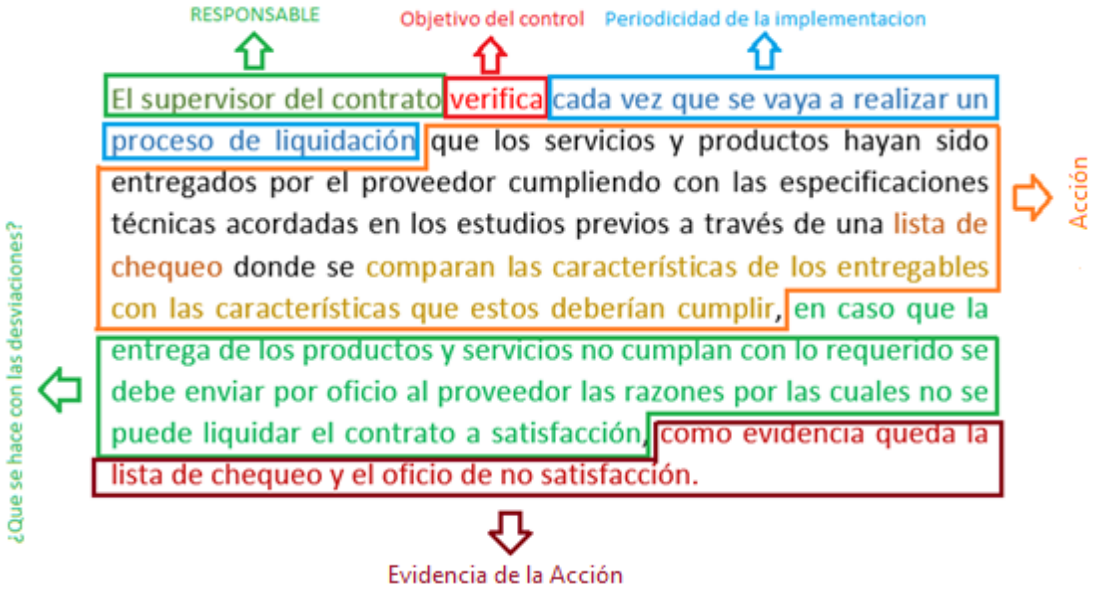
- Debe tener un **responsable** de su ejecución (evitar colocar áreas generales o nombres propios), por ejemplo: responsable de inventarios.
- La ejecución del control **debe tener un soporte documental**, por ejemplo, una base de datos, una lista de chequeo, un acta de reunión, etc.
- En la descripción 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.

Nota:

- *Se solicitará el Cargue cuatrimestral de evidencias para todos los controles, para aquellos casos en los cuales la periodicidad de ejecución de la actividad sea superior a la fecha de cargue de evidencias se deberá adjuntar un soporte que permita verificar los avances o proyección de ejecución de la actividad control*
- *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. Dicha información debe ser acorde a lo dictaminado en la Ley 1712 del 2014 y lo desarrollado en el "Índice de Información Clasificada y Reservada" de la entidad.*

- *Se recomendará el uso de Matrices gerenciales para los casos en los cuales se presente manejo de información reservada o clasificada, con las cuales se logre evidenciar la ejecución de las actividades control.*
- *La manera en la cual se lleva a cabo su implementación 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.*
- *Cada causa del riesgo debe tener **por lo menos un control** asignado a su mitigación.*

La siguiente es la estructura para los controles recomendada.



Fuente: Elaboración Propia

Para el Riesgo de SARLAFT se estructuran controles con el siguiente enfoque:

- Evitar que se introduzcan recursos de actividades ilícitas a través de la entidad, identificando la fuente del riesgo y quien lo genera, para fortalecer el esquema de prevención. (Preventivo)
- Identificar señales de alerta que se generan por un número de hechos que sumados se salen del normal desarrollo económico y se convierte en una operación inusual, que debe evaluarse para determinar su reporte como una operación sospechosa de UIAF. (Detectivo)
- Política de conocimiento de los clientes, de los empleados, de proveedores, contratistas u otros. (Preventivo)
- Política de segmentación de mercado que contempla a los clientes, productos, canales de distribución y jurisdicciones. (Preventivo)
- Política sobre los productos ofrecidos. (Preventivo)

- Política de conocimiento, capacitación y ambiente antilavado en la entidad. (Preventivo)
- Política de control respecto de los agentes generadores de riesgo. (Preventivo)
- Política de manejo de recursos en efectivo en la entidad. (Preventivo)
- Política de monitoreo de la información respecto de los factores de riesgo. (Preventivo)
- Política de conservación de documentos. (Preventivo)
- Política de cumplimiento de las funciones frente al SARLAFT(Preventivo)
- Implementación de listas restrictivas o vinculantes que relacionan a las personas naturales y jurídicas, que pueden estar vinculadas con actividades de LA/FT (Detectivo)
- Seguimiento de varias fuentes de información como noticias en prensa, listas vinculantes y otras fuentes del sector, para el monitoreo de las contrapartes donde puede estar relacionado un tercero vinculado. (Detectivo)
- Verificación de la vinculación de un tercero, establecido en la política de la entidad, señalando que la información de los clientes y/o usuarios debe actualizarse mínimo cada año. (Detectivo)

11.8 Etapa 8: Calificación del control

Una vez se haya estructurado el control se debe pasar a una etapa de calificación de su efectividad en la tarea de mitigar el riesgo, para esto se debe presentar una evaluación del control con base en el análisis de las características presentadas**.** 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.

A continuación, se presentan los criterios para calificar la efectividad del control, con ello se busca obtener una calificación de 0 a 100, en cumplimiento de las características mencionadas en el numeral antes mencionado, cada respuesta tiene un peso específico y no pueden existir respuestas diferentes a las relacionadas:

Criterio de evaluación.	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del Responsable.	Asignado	15
	No Asignado	0
1.2 Segregación y Autoridad del Responsable.	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un Control	0
4. Como se realiza la actividad de control.	Confiable	15
	No Confiable	0
5. Que pasa con las observaciones o desviaciones.	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente.	0
6. Evidencia de la ejecución del control.	Completa	10
	Incompleta	5
	No Existe	0

59

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

Se debe resaltar que no solo basta con que el control esté debidamente diseñado, sino también se tiene que velar que su implementación y ejecución sea la adecuada.

Inicialmente la Determinación de Ejecución del Control será una confirmación por parte del responsable del proceso, y posteriormente se debe ratificar con el cargue de las evidencias de las actividades de control en los periodos de corte establecidos dentro de la presente Política, de lo cual el Profesional de la Administración de Riesgos de la Oficina Asesora de Planeación elaborará un Informe de Seguimiento al vencimiento de cada periodo que a su vez será evaluado por Control Interno o Auditoría Interna.

Continuando con los criterios de Evaluación del Control, se establecerá 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.

60

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

Una vez se tienen las dos calificaciones se ponderan para dar la calificación de solidez individual que se especifica en la siguiente tabla para definir si se hace necesaria la aplicación de un plan de acción para fortalecer el control:

Peso del diseño individual o promedio de los Controles. (DISEÑO)	El Control se ejecuta de manera consistente por los responsables. (EJECUCION)	Solidez individual de cada control Fuerte:100 Moderado:50 Debil:0	Aplica plan de acción para fortalecer el Control Si / NO
Fuerte Calificación Entre 96 y 100	**Fuerte** (Siempre se ejecuta)	Fuerte + Fuerte = Fuerte	No
	Moderado (Algunas veces)	Fuerte + Moderado = Moderado	Si
	Débil (No se ejecuta)	Fuerte + Débil = Débil	Si
Moderado Calificación Entre 86 y 95	**Fuerte** (Siempre se ejecuta)	Moderado + Fuerte = Moderado	Si
	Moderado (Algunas veces)	Moderado + Moderado = Moderado	Si
	Débil (No se ejecuta)	Moderado + Débil = Débil	Si
Débil Entre 0 y 85	**Fuerte** (Siempre se ejecuta)	Débil + Fuerte = Débil	Si
	Moderado (Algunas veces)	Débil + Moderado = Débil	Si
	Débil (No se ejecuta)	Débil + Débil = Débil	Si

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

Si hay más de un control que mitiga una causa estos dos se promedian para verificar cual es la solidez del promedio de los controles de la siguiente manera:

Calificación de la Solidez del conjunto de controles.	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

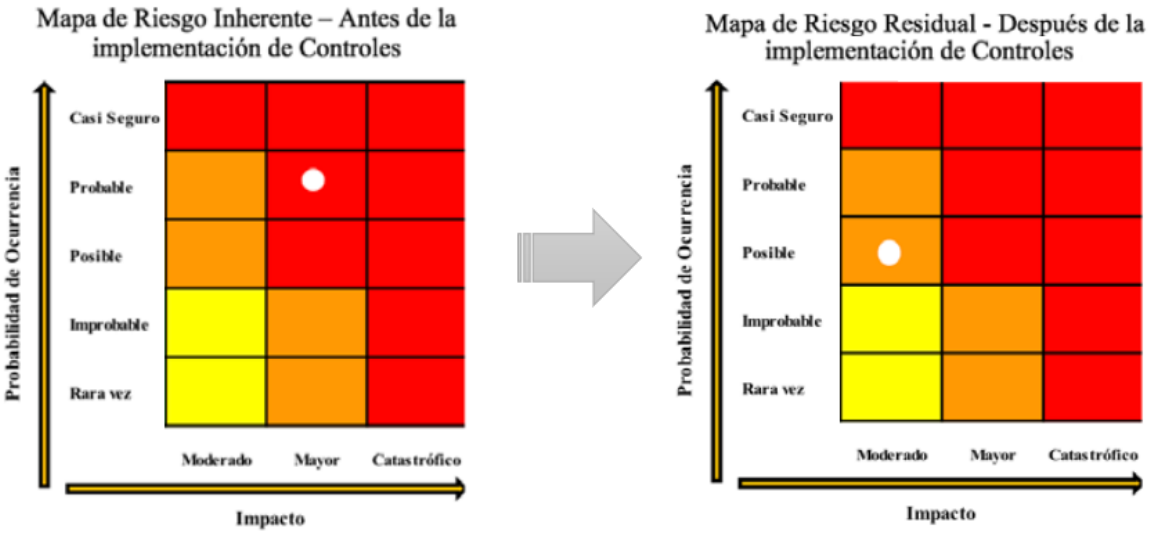
11.9 Etapa 9: Nivel de riesgo residual

Una vez se tiene esta calificación de solidez de los controles se determina la lógica con la cual el nivel del riesgo residual se va a desplazar en el mapa de calor para el Riesgo de Corrupción lo cual se detalla a continuación:

Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.				
Solidez del conjunto de los controles.	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir Impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la Probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de Impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No Disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No Disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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. El desplazamiento en el Mapa de Calor debe ser similar a la siguiente, siempre propendiendo una disminución en la Zona de Riesgo.



Fuente: Elaboración Propia

11.10 Etapa 10: 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:

- **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.

Se aclara que no existe zona de Riesgo residual Bajo, de tal forma todos los Riesgos deben contar con un Tratamiento diferente a Aceptar el Riesgo.

Todo Riesgos de Corrupción y SARLAFT debe contar con un Indicador, Formula y Meta. Para estos últimos los indicadores deben ir dirigidos a la Probabilidad e Impacto de las fuentes de Riesgo.

11.11 Etapa 11: Reporte de Operaciones Sospechosas

Uno de los propósitos de la gestión de Riesgos de SARLAFT es identificar las actividades, hechos y operaciones, que por sus características no son razonables respecto de una actividad económica o sector y que las hace sospechosas.

Para ello la entidad da cumplimiento a las políticas del sistema SARLAFT, ejecutando lo siguiente:

- Comprobar
- Supervisar
- Observar críticamente
- Registrar los procesos derivados de una nueva actividad, acción o sistema.
- Evidenciar cambios significativos.

Con lo anterior se permite la identificación las operaciones inusuales que se generaron en el proceso de monitoreo respecto a los controles detectivos y que sugieren evaluarse. De tal forma que el sistema SARLAFT, deberá detectar las operaciones inusuales con base en el registro de clientes, usuarios, Personas Públicamente Expuestas (PEP's), proveedores y la existencia de cambios atípicos en las operaciones como las zonas, los montos y el número de transacciones relacionadas con los productos, bienes o servicios ofrecidos por la entidad.

Las operaciones inusuales se analizan y se determina el criterio objetivo con en el que se le otorga la característica de sospechosa respecto a LA/FT catalogándolas como importantes y significativas por su grado de complejidad, debido a que se salen de los patrones habituales sin fundamento económico a fin de remitirlas a la UIAF de manera oportuna.

El Reporte de Operaciones Sospechosas (ROS) constituye información útil y pertinente para que la UIAF pueda realizar inteligencia financiera y detectar señales indicativas de LA/FT, para darlas a conocer a la autoridad competente en la investigación penal de los delitos.

Las señales de alerta permiten que, en el desarrollo de las actividades derivadas de las funciones de la entidad, los servidores de cualquier nivel puedan identificar operaciones sospechosas de LA/FT ya su vez las puedan reportar. En caso de que algún funcionario detecte señales de alerta, deberá reportarlas al buzón SARLAFT el cual también está disponible para la ciudadanía.

11.11.1 Características del Reporte de Operaciones Sospechosas

El Reporte de Operaciones Sospechosas (ROS) es el medio de comunicación dirigido a la UIAF que como autoridad competente será notificada de las operaciones que representan riesgo de LA/FT en la entidad.

El ROS cuenta con una variedad de características, entre ellas:

- **Se debe reportar de manera inmediata a la UIAF**. Tan pronto como se determina una operación como sospechosa, en cumpliendo con los lineamentos establecidos por la entidad receptora. Este se constituye como el medio por el cual los sujetos obligados y los no obligados que aplican buenas prácticas, comunican a la UIAF los detalles de las operaciones detectadas como sospechosas.
- **No se constituye en una denuncia penal. E**s decir que no es necesario tener exactitud de que se trata de una actividad delictiva o la identificación del tipo penal o que los recursos obtenidos provienen directamente de actividades delictivas.
  El artículo 42 de la Ley 190 de 1995 detalla que los ROS enviados a la UIAF no constituyen una denuncia ni dan lugar a ningún tipo de responsabilidades para la entidad, ni para las personas que hayan participado en su detección o reporte.
- **La obligación de reportar operaciones sospechosas a la UIAF no exime de la obligación de denunciar si es el caso ante las entidades competentes.** Los delitos que se adviertan en el ejercicio de las funciones o de emprender acciones

para perseguir eventuales responsabilidades administrativas cuando corresponda es deber del funcionario como Ciudadano.

- Es un elemento fundamental para iniciar las acciones de las autoridades competentes en LA/FT, por lo que la claridad que acompaña su contenido incide en la manera de interpretar los hechos asociados al LA/FT y por ende la evaluación realizada por la UIAF.
- **Es confidencial,** está protegido por la reserva legal entre la entidad y la UIAF, esto se refiere a que los reportes no harán parte de expedientes ni como anexos de la información entregada por la UIAF a las autoridades competentes.

Cabe destacar que los reportes del ROS deben cumplir con los parámetros fijados por la UIAF en el formato establecido. Para ello se encuentra el instructivo ROS publicado en la página web www.uiaf.gov.co en la sección Reportantes (en cada sector al que pertenece la entidad reportante).

12. IDENTIFICACIÓN Y GESTIÓN DEL RIESGO (RIESGO SEG. DE LA INFORMACIÓN)

En la Secretaria 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, así:

12.1 Etapa 1: Conocimiento de la actual Política de Administración de Riesgos

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 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 - políticas, lineamientos y manuales - Plan estratégicos sectoriales e instituciones- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

12.2 Etapa 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 Secretaria Distrital de Seguridad convivencia y Justicia acorde a la Guía de Gestión de Activos de Información -G-FD-1, los cuales deben ser clasificados y valorados teniendo en cuenta que en el contexto de seguridad de la información, estos se refieren a: Hardware, software, aplicaciones de la Entidad, servicios web, redes, información digital, personal, ubicación, organización,, TI (Tecnologías de la Información), TO (Tecnologías de la Operación) 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 de **Recursos físicos y documental**, de acuerdo con los siguientes pasos, así:

12.2.1 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 y Gestión Documental y los líderes de los procesos teniendo en cuenta los siguiente:

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC

a. Listar los activos de información por cada proceso

Registrar los activos de información de acuerdo con lo definido en la Guía de Gestión de Activos de Información G-FD-1 en el formato Registro de Activos de Información - F-FD-513.

b. Identificar el dueño de los activos:

En la identificación de los responsables de los activos de información, es importante definir los garantes del cuidado, protección y conservación de estos, lo cual se realizará en el formato Registro de Activos de Información F-FD-513, por lo general está a cargo del líder del proceso o jefe de áreas, o quienes ellos asignen.

c. Clasificar los activos

Los activos de la Entidad se clasifican en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada de acuerdo con lo definido en la Guía de Gestión de Activos de Información -G-FD-1 de la Entidad, la cual está acorde a lo determinado por el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC.

1. Información
2. Software
3. Recurso Humano
4. Servicio
5. Hardware
6. Otros

d. Clasificar 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 dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.

e. Determinar la criticidad del activo (Valoración del Activo)

Evaluar la criticidad de los activos de la Secretaria 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.

f. Identificar si existen 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

Fuente: Modelo de Gestión de Riesgos de Seguridad Digital-MINTIC

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 - Dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013

12.3 Etapa 3: 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 que pueden hacer daño a los activos de la Entidad, materializar los riesgos y generar algunas vulnerabilidades (debilidades):

Tabla Amenazas comunes

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**
	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**
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**
Acciones no autorizadas	Uso no autorizado del equipo	**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**
Compromiso de las funciones	Error en el uso	**D, E**
	Abuso de derechos	**D, E**

TIPO	AMENAZA	ORIGEN
	Falsificación de derechos	**D**
	Negación de acciones	**D, E**
	Incumplimiento en la disponibilidad del personal	**D, E**

Fuente: ISO/IEC 27005:2009

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

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

Tabla Amenazas dirigida por el Hombre

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

Fuente: ISO/IEC 27005:2009

Identificación de vulnerabilidades: Se puede identificar vulnerabilidades (debilidades), de acuerdo con el tipo de activo:

Tabla Vulnerabilidades comunes

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.
Software	Ausencia o insuficiencia de pruebas de software.	Abuso de derechos.

Tipos	Ejemplo de vulnerabilidad	Ejemplo de Amenaza
	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.
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.

Tipos	Ejemplo de vulnerabilidad	Ejemplo de Amenaza
	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.
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.
	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.

Tipos	Ejemplo de vulnerabilidad	Ejemplo de Amenaza
	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.
	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.

Fuente: 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.

Tabla de amenazas y vulnerabilidades de acuerdo con el 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

Fuente: ISO/IEC 27005:2009

12.4 Etapa 4: Valoración del riesgo

La valoración del riesgo de seguridad de la Información en la Secretaria Distrital de Seguridad, Convivencia y Justicia, se ajusta de acuerdo con lo establecido en el numeral 5.3 de la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 – 2020 del Departamento Administrativo de la Función Pública **DAFP.**

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

Tabla Criterio de Probabilidad

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%

Fuente: Oficina Asesora de Planeación Secretaria Distrital de Seguridad, Convivencia y Justicia.

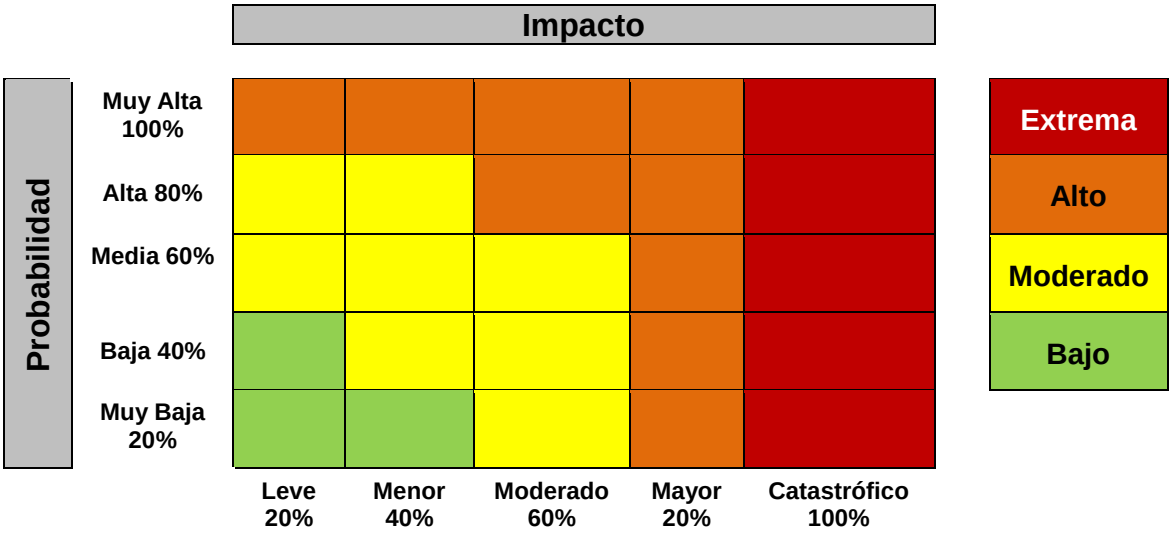
De igual forma para determinar el impacto económico y reputacional se cuenta con la siguiente tabla que es valorada por niveles de la siguiente forma:

Tabla Criterio de impacto

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%
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%

Fuente: Oficina Asesora de Planeación Secretaria 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):



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicasV.5

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 del proceso 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.

12.5 Etapa 5: 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 10.7** creación de controles del presente documento.

12.6 Etapa 6: 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.

12.7 Etapa 7: Monitoreo, revisión y reporte de la Gestión de Riesgos de Seguridad de la Información

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.

El responsable de realizar el seguimiento a los riesgos de seguridad de la Información debe reportar cuatrimestralmente a la mesa técnica de Seguridad Digital.

Detalles adicionales se presentan en el numeral **15.4** del presente documento

13. IDENTIFICACIÓN Y GESTIÓN DEL RIESGO (RIESGOS ESTRATEGICOS)

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.

13.1 Etapa 1: Conocimiento de la actual Política de Administración de Riesgos y Divulgación de la Matriz de Riesgos Estratégicos

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:

Intranet: Lineamientos y normatividad - Transparencia (planes - matriz de riesgo) - Planes Estratégicos, Sectoriales e Institucionales - Plan Estratégico Institucional
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

13.2 Etapa 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) tanto para el nivel de Riesgo Inherente como para el nivel de Riesgo Residual.
- Los controles están a cargo del proceso de Direccionamiento Sectorial e Institucional propendiendo el seguimiento a las actividades desde la ejecución de los proyectos de inversión y 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 le efectuará la Evaluación global de los controles establecida en el numeral **11.8**
- El ejercicio culminará con estructura del indicador de cumplimiento.

13.3 Etapa 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 **11.9**.

14. 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, para el segundo de los casos es decir las **oportunidades**, se entenderá para potenciales afectaciones que pudieren generar un impacto positivo.

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**, la cual se describe a continuación:

14.1 Etapa 1: Identificación de Oportunidades

El insumo principal para la identificación de oportunidades será la matriz DOFA del proceso, de donde se identifican las Oportunidades establecidas allí y que son entendidas como situaciones externas favorables a la organización, en este sentido previamente, se debe valorar si las oportunidades presentan afinidad, así las cosas, si se cuenta con 5 oportunidades, éstas podrían resumirse en una sola o en dos, esta situación solo se podrá dar si hace un análisis de afinidad entre las mismas, en caso de no poderse agrupar por afinidad, se debe hacer una valoración de cuales de las oportunidades son relevantes y solo en este momento ya fuese por afinidad o selección de las oportunidades relevantes, se da inicio a la construcción de la matriz.

Como mínimo cada proceso debe presentar una oportunidad, no obstante, si evaluada la DOFA del proceso, se identifican otras oportunidades que no se han contemplado, estas podrán solicitarse al proceso para su incorporación.

En caso de que se establezca más de una oportunidad, estas deben analizarse en filas independientes, tal y como se muestra a continuación:

No OP	Proceso	Oportunidad
1	Direccionamiento sectorial e institucional	Oportunidad 1
2	Direccionamiento sectorial e institucional	Oportunidad 2

Fuente: Elaboración propia

Nota1: Estas son las tres primeras columnas de la Matriz de identificación, calificación y seguimiento de oportunidades institucionales.
Nota 2: Las oportunidades se deben redactar de manera positiva.

14.2 Etapa 2: Calificación De Oportunidades

Al igual que los riesgos, las oportunidades se califican a través de probabilidad e impacto, para ello se entenderá por cada uno lo siguiente:

Probabilidad: posibilidad de ocurrencia de la oportunidad, para ello se tendrán las siguientes escalas:

- No se ha presentado en los últimos 5 años, en este sentido la selección de esta opción asigna un puntaje de 1.
- Se presento al menos una vez en los último 5 años, en este sentido la selección de esta opción asigna un puntaje de 2.
- Se Presento al menos una vez en los últimos 2 años, en este sentido la selección de esta opción asigna un puntaje de 3.
- Se Presento al menos una vez en el último año, en este sentido la selección de esta opción asigna un puntaje de 4.
- Se ha presentado más de una vez en el año, en este sentido la selección de esta opción asigna un puntaje de 5.

Impacto: Beneficios resultantes de la posible materialización de la oportunidad

- Cumplimiento de las metas y objetivos institucionales favoreciendo la realización de las metas de gobierno y/o Imagen institucional favorecida en el orden nacional o regional por cumplimientos en la prestación del servicio a los usuarios o ciudadanos, en este sentido la selección de esta opción asigna un puntaje de 5.
- Mejoramiento en la calidad del servicio y satisfacción de los grupos de valor, en este sentido la selección de esta opción asigna un puntaje de 4.
- Aportes parciales al cumplimiento de las metas y objetivos institucionales, en este sentido la selección de esta opción asigna un puntaje de 3.
- Aporte mínimo al mejoramiento en la calidad de los servicios y satisfacción de los usuarios, en este sentido la selección de esta opción asigna un puntaje de 2.
- Sin aportes al cumplimiento de las metas y objetivos institucionales, el mejoramiento y satisfacción de los usuarios, en este sentido la selección de esta opción asigna un puntaje de 1.

En este sentido, se deben diligenciar los siguientes campos:

No Op	Proceso	Oportunidad	Probabilidad (de lograr la oportunidad)		Evidencia de la probabilidad	Impacto (Beneficios obtenidos con la oportunidad)		Factor de la oportunidad (Probabilidad x Beneficio)
			Probabilidad	Calificación probabilidad		Impacto	Calificación del impacto	

Fuente: Elaboración Propia

Nota1: La probabilidad y el impacto se seleccionan de una lista desplegable, la calificación de la probabilidad se genera de manera automática.
Nota 2: Cuando se califique la probabilidad, en el campo de evidencia de la probabilidad, se debe colocar la evidencia objetiva que soporta la frecuencia de la probabilidad seleccionada.
Nota 3: El factor de oportunidad, es un valor automático, que sale de la relación obtenida entre la calificación de la probabilidad y la calificación del impacto.

14.3 Etapa 3: Escenario de Intervención

El escenario de intervención será resultante de multiplicación de la probabilidad por el impacto, con lo cual aparecerá el escenario de intervención de oportunidad, para ello se tendrá en cuenta lo siguiente:

- Si el factor de oportunidad presenta un valor mayor a 15, el plan de acción de la actividad debe desarrollarse de manera inmediata o en un plazo menor a seis meses.
- Si el factor de oportunidad presenta un valor entre 10 y 15, el plan de acción de la actividad debe desarrollarse en mediano plazo, es decir entre seis meses y un año.
- Si el factor de oportunidad presenta un valor entre 5 y 9, el plan de acción de la actividad debe desarrollarse en largo plazo, es decir entre un año y dos años.
- Si el factor de oportunidad presenta un valor menor a 5, el plan de acción de la actividad debe desarrollarse en un plazo mayor a dos años o se debe tomar la decisión de no efectuar nada.

Factor de la oportunidad (Probabilidad x Beneficio)	Escenario de intervención de la oportunidad	Actividad que se realizará	¿La actividad es técnica, financiera y jurídicamente viable? (Si la respuesta es SI a las tres opciones continúe a las siguientes columnas, si la respuesta es NO a una o a las tres opciones, replantee la actividad que se plantea realizar)
15	ACCIONES Y ACTIVIDADES A MEDIANO PLAZO (MAYOR A SEIS MESES)	Realizar convenio con el DANE para obtención de plataforma tecnológica	SI

Fuente: Elaboración propia

Nota 1: La actividad a realizar debe corresponder a una acción objetiva, es decir que pueda ser evidenciable en su cumplimiento.
Nota 2: Es fundamental que la actividad que se pretenda realizar, presente tanto viabilidad técnica, financiera y jurídica, en este sentido en la columna que evalúa las viabilidades, en caso de que la respuesta fuese NO, se debe formular otra actividad, que permita dar cumplimiento a las tres viabilidades, y solo hasta que la respuesta seleccionada corresponda al SI, se podrá seguir con las siguientes columnas.

14.4 Etapa 4: Desarrollo de la actividad

Las últimas cuatro columnas de la matriz corresponden al período en el cual se desarrollará la actividad, así como la evidencia del seguimiento y la determinación del beneficio real.

Fecha inicio (DD/MM/AA)	Fecha fin (DD/MM/AA)	Evidencia del seguimiento	Verificación ¿Hay éxito post implementación? ¿Cuál?
1/03/2019	30/10/2019	Sistema de información operando en la entidad	La información se consolida en tiempo real

Fuente: Elaboración propia

Nota 1: Las fechas en las cuales se desarrollarán las actividades, se relacionarán en el formato DD/MM/AA, es necesario que este período corresponda al escenario de intervención de la oportunidad, es decir, se debe tener en cuenta si la intervención es inmediata, o del corto, mediano y largo plazo, en caso de que el escenario de intervención es mayor a dos años, se debe colocar N.A., tanto en la fecha de inicio, como la de fin.
Nota 2: La evidencia del seguimiento, es un documento que debe dar fe de la realización de la actividad.
Nota 3: Cuando de manera inmediata se pueda establecer evidencia del éxito esta debe colocarse en el campo de verificación, esta situación se comprobará a través de la auditoría interna, en caso de que no se presente una mejora inmediata se colocará N.A., sin embargo, en futuras auditorías se comprobará el éxito de esta.

Una vez ha sido estructurada por los líderes de los procesos, esta debe remitirse a la Oficina de Planeación, quien será la encargada de la consolidación respectiva.

15. PUBLICACIÓN, SEGUIMIENTO Y EVALUACIÓN A LOS RIESGOS

En cumplimiento de lo consignado en el MIPG y con el objetivo de implementar un monitoreo efectivo para la adecuada administración de los riesgos en la SDSCJ, corresponde a los líderes de procesos y líderes operativos realizar la revisión y seguimiento de sus respectivos mapas de riesgos ejercicio que debe ser continúo y permanente.

Una vez desarrollado lo consignado en la presente Política, el profesional designado para la gestión de los riesgos por parte de la Oficina Asesora de Planeación recopila los riesgos identificados y procederá la agrupación de todos los Riesgos en las Matrices destinadas para ello y de esta forma se procederá con la publicación y divulgación. No obstante, todo riesgo de debe ser aprobado por el líder de proceso y gestionado por el Líder operativo. La versión Vigente de las Matrices será la última publicada tanto en la Página WEB como en la Intranet de la entidad, lo cual debe estar respaldado por lo compilado en el sistema Portal MIPG que administra la Oficina Asesora de Planeación.

Para información referente al diligenciamiento de la Matriz de Riesgos por Procesos, Riesgos por Corrupción, Riesgos de Seguridad de la Información y Matriz de Oportunidades por favor ponerse en contacto con el Profesional de Riesgos designado por la Oficina Asesora de Planeación y de Seguridad de la Información de la Dirección de Tecnologías y Sistemas de la Información respectivamente. Los resultados de los Informes de Seguimiento y evaluación serán socializados y divulgados en el Comité Institucional de Coordinación de Control Interno.

15.1 Seguimiento a la Matriz de Riesgos por Procesos Institucional F-DS-575

Es responsabilidad de la segunda línea de defensa realizar el seguimiento a la Matriz de Riesgos por Procesos Institucional de manera trimestral, con un plazo de 10 días hábiles, una vez vencido el trimestre, para presentar un informe de gestión al jefe de la Oficina Asesora de Planeación y al Jefe de la Oficina de Control Interno, responsable de la tercera línea de defensa.

Para cumplir con el anterior plazo descrito se requiere que los Líderes Operativos realicen el cargue de las evidencias a más tardar el 5° día hábil luego de vencido el Trimestre. Cualquier evidencia ubicada luego de dicho termino no se contemplará en la seguimiento y evaluación.

Las actividades y el responsable se detallan a continuación:

ACTIVIDAD	RESPONSABLE
Revisión de la implementación de los controles y los eventos de riesgo del proceso	Líder operativo del proceso

Cargue de soportes documentales de la implementación de los controles	Líder operativo del proceso
Revisión de los soportes documentales de la implementación de los controles	Encargado de la gestión de riesgos de la OAP
Envió del informe de seguimiento a la matriz de riesgos por proceso	Encargado de la gestión de riesgos de la OAP

Fuente: Elaboración propia

En este reporte de seguimiento se debe analizar si los soportes documentales de la ejecución de los controles reportados por el líder operativo realmente corresponden a los soportes documentales que están estructurados en la matriz de riesgos por proceso, en otras palabras, se debe determinar si los controles efectivamente se ejecutaron con el objetivo de mitigar los riesgos en cada uno de los procesos respectivos.

15.2 Seguimiento a la Matriz de Corrupción Institucional F-DS-578

Es responsabilidad de la segunda línea de defensa realizar el seguimiento a la Matriz de Riesgos por Corrupción Institucional de manera cuatrimestral, con un plazo de 5 días hábiles, una vez vencido el cuatrimestre, para presentar un informe de gestión al jefe de la Oficina Asesora de Planeación y al Jefe de la Oficina de Control Interno, responsable de la tercera línea de defensa. El anterior incluirá las mejoras o ajustes realizados a los Riesgos o controles durante el periodo.

Para cumplir con el anterior plazo descrito se requiere que los Líderes Operativos realicen el cargue de las evidencias a más tardar el 3° día hábil luego de vencido el Cuatrimestre. Cualquier evidencia ubicada luego de dicho termino no se contemplará en la seguimiento y evaluación.

Las actividades y el responsable se detallan a continuación:

ACTIVIDAD	RESPONSABLE
Revisión de la implementación de los controles y los eventos de riesgo de corrupción	Líder operativo del proceso
Cargue de soportes documentales de la implementación de los controles	Líder operativo del proceso
Revisión de los soportes documentales de la implementación de los controles	Encargado de la gestión de riesgos de la OAP
Envió del informe de seguimiento a la matriz de riesgos de corrupción	Encargado de la gestión de riesgos de la OAP

Fuente: Elaboración propia

En este reporte de seguimiento se debe analizar si los soportes documentales de la ejecución de los controles reportados por el líder operativo realmente corresponden a los soportes documentales que están estructurados en la matriz de riesgos de corrupción, en otras palabras, se debe determinar si los controles efectivamente se ejecutaron con el objetivo de mitigar los riesgos en cada uno de los procesos respectivos.

15.3 Seguimiento a la matriz de Seguridad digital F-DS-898

Es responsabilidad del profesional de Seguridad de la Información de la Dirección de Tecnologías y Sistemas de la Información, realizar el seguimiento a la Matriz de Riesgos de Seguridad de la Información de manera cuatrimestral con el acompañamiento de la Oficina Asesora de Planeación, con un plazo de 10 días hábiles, una vez vencido el cuatrimestre, presentará un informe de gestión a la Oficina de Control Interno, responsable de la tercera línea de defensa.

Para cumplir con el anterior plazo descrito se requiere que los Líderes Operativos realicen el cargue de las evidencias a más tardar el 5° día hábil luego de vencido el Cuatrimestre. Cualquier evidencia ubicada luego de dicho termino no se contemplará en la seguimiento y evaluación.

Las actividades y el responsable se detallan a continuación:

ACTIVIDAD	RESPONSABLE
Revisión de la implementación de los controles y los eventos de riesgo de Seguridad de la información	Líder operativo del proceso
Cargue de soportes documentales de la implementación de los controles	Líder operativo del proceso
Revisión de los soportes documentales de la implementación de los controles	Encargado de la gestión de riesgos de la DTSI
Envió del informe de seguimiento a la matriz de riesgos de Seguridad de la Información	Encargado de la gestión de riesgos de la DTSI

Fuente: Elaboración propia

En este reporte de seguimiento se debe analizar si los soportes documentales de la ejecución de los controles reportados por el líder operativo realmente corresponden a los soportes documentales que están estructurados en la matriz de riesgos de Seguridad Digital, en otras palabras, se debe determinar si los controles efectivamente se ejecutaron con el objetivo de mitigar los riesgos en cada uno de los procesos respectivos.

15.4 Seguimiento a la matriz de Oportunidades institucional F-DS-576

Es responsabilidad de la segunda línea de defensa realizar el seguimiento a la Matriz De Identificación, Calificación Y Seguimiento De Oportunidades Institucionales de manera semestral, con un plazo de 15 días hábiles, una vez vencido el semestre, para presentar un informe de gestión al jefe de la Oficina Asesora de Planeación y al Jefe de la Oficina de Control Interno, responsable de la tercera línea de defensa.

Para cumplir con el anterior plazo descrito se requiere que los Líderes Operativos realicen el cargue de las evidencias a más tardar el 10° día hábil luego de vencido el Semestre. Cualquier evidencia ubicada luego de dicho termino no se contemplará en la seguimiento y evaluación.

Las actividades y el responsable se detallan a continuación:

ACTIVIDAD	RESPONSABLE
Revisión de la ejecución de Oportunidades	Líder operativo del proceso
Cargue de soportes documentales de la ejecución de Oportunidades	Líder operativo del proceso
Revisión de los soportes documentales de la ejecución de los Oportunidades	Encargado de la gestión de riesgos de la OAP
Envió del informe de seguimiento a la matriz de Oportunidades	Encargado de la gestión de riesgos de la OAP

Fuente: Elaboración propia

En este reporte de seguimiento se debe analizar si los soportes documentales de la ejecución reportado por el líder operativo realmente corresponden a los soportes documentales que están estructurados en la matriz de Oportunidades, en otras palabras, se debe determinar si los controles efectivamente se ejecutaron en cada uno de los procesos respectivos.

15.5 Seguimiento a la Matriz de Riesgos Estratégicos F-DS-573

Es responsabilidad de la segunda línea de defensa realizar el seguimiento a la Matriz de Riesgos Estratégicos de manera semestral, con un plazo de 15 días hábiles, una vez vencido el Semestre, para presentar un informe de gestión al jefe de la Oficina Asesora de Planeación y al Jefe de la Oficina de Control Interno, responsable de la tercera línea de defensa.

Para cumplir con el plazo anteriormente descrito, se requiere que el área de Proyectos de Inversión de la Oficina de planeación realice el cargue de las evidencias a más tardar el 10° día hábil luego de vencido el Semestre. Cualquier evidencia ubicada luego de dicho termino no se contemplará en la seguimiento y evaluación.

Las actividades y el responsable se detallan a continuación:

ACTIVIDAD	RESPONSABLE
Revisión de la implementación de los controles y los eventos de riesgo estratégicos	área de Proyectos de Inversión de la Oficina de planeación
Cargue de soportes documentales de la implementación de los controles	área de Proyectos de Inversión de la Oficina de planeación
Revisión de los soportes documentales de la implementación de los controles	Encargado de la gestión de riesgos de la OAP
Envió del informe de seguimiento a la matriz de riesgos estratégicos	Encargado de la gestión de riesgos de la OAP

Fuente: Elaboración propia

En este reporte de seguimiento se debe analizar si los soportes documentales de la ejecución de los controles reportados por el líder operativo realmente corresponden a los soportes documentales que están estructurados en la matriz de riesgos estratégicos, en otras palabras, se debe determinar si los controles efectivamente se ejecutaron con el objetivo de mitigar los riesgos en cada uno de los procesos respectivos.

15.6 Evaluación de las matrices de riesgo

Es responsabilidad de la tercera línea de defensa la evaluación de las matrices de riesgo, verificando que la información que reposa en estos dos documentos cumpla con los lineamientos expresados en esta política. En caso de encontrar desviaciones entre dicha información y el deber ser se podrán generar acciones de mejora, las cuales seguirán los lineamientos de ejecución dictados por la Oficina de Control Interno.

Adicionalmente, otra de las responsabilidades de la tercera línea de defensa es la de verificar el reporte de seguimiento realizado por la segunda línea de defensa, con base a las evidencias depositadas de la ejecución de controles para los riesgos y oportunidades reportados por los líderes operativos en concordancia con lo depositado en las Matrices y lo soportado en la carpeta SharePoint administrada por la Oficina Asesora de Planeación, con base en esta estimación se puede emitir una sugerencia al proceso correspondiente para que el control o actividad de oportunidad sea modificada con el objetivo de mejorar su efectividad.

Los cortes para el seguimiento al mapa de riesgos por **Proceso** se muestran a continuación:

FECHA DE CORTE	ENTREGA DEL INFORME
Primer corte: 31 de marzo	Segunda semana de mayo
Segunda corte: 30 de junio	Segunda semana de agosto
Tercer corte: 30 de septiembre	Segunda semana de noviembre
Cuarto corte: 31 de diciembre	Segunda semana de febrero

Fuente: Elaboración propia

Los cortes para realizar el seguimiento a la matriz de riesgos de **Corrupción** son los siguientes:

FECHA DE CORTE	ENTREGA DEL INFORME
Primer corte: 30 de abril	A los 10 días hábiles de mayo
Segunda corte: 31 de agosto	A los 10 días hábiles de septiembre
Tercer corte: 31 de diciembre	A los 10 días hábiles de enero

Fuente: Elaboración propia

Los cortes para realizar el seguimiento a la matriz de riesgos de **Seguridad de la Información** una vez se encuentre formulada, publicada, socializada e implementada son los siguientes:

FECHA DE CORTE	ENTREGA DEL INFORME
Primer corte: 30 de abril	Segunda semana de mayo
Segunda corte: 31 de agosto	Segunda semana de octubre
Tercer corte: 31 de diciembre	Segunda semana de febrero

Fuente: Elaboración propia

Los cortes para el seguimiento al mapa de **Oportunidades** se muestran a continuación:

FECHA DE CORTE	ENTREGA DEL INFORME
Único corte a 31 de diciembre	Según el Plan Anual de Auditoría

Fuente: Elaboración propia

Los cortes para el seguimiento al mapa de **Estratégicos** se muestran a continuación:

FECHA DE CORTE	ENTREGA DEL INFORME
Primer corte: 30 de junio	Cuarta semana de agosto
Segundo corte: 31 de diciembre	Cuarta semana de febrero

Fuente: Elaboración propia

Cabe resaltar que los seguimientos y evaluaciones se efectuaran siempre y cuando existan Riesgos reportados para efectuar los respectivos.

Todo lo contemplado en la presente Política queda sujeto al ejercicio auditor que podrá desarrollarse interna o externamente propendiendo la mejora continua de la Entidad.

16. BIBLIOGRAFÍA

Departamento Administrativo de la Función Pública. (2020). *Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas. Riesgos de gestion, corrupcion y seguridad digital. Version 5.* Bogotá D.C: Dirección de Control Interno y Racionalización de Tramites

Ruta Metodologica para la Implementacion del SARLAFT en las Entidades Distritales. (2020). Secretaria General de la alcaldia Mayor de Bogota D.C.

Alcaldía Mayor de Bogotá. (28 de 12 de 2011). *NTD-SIG 001:2011.* Obtenido de Sistema Integrado de Gestión Distrital: http://portel.bogota.gov.co/secretariageneral/dddi/educacion/docs/anexo_decreto_652_2011_ntdsig.pdf

Presidencia de la República. (2015). *Guía para la Gestión del Riesgo de Corrupción .* Bogotá D.C.

Presidencia de la República de Colombia. (21 de 05 de 2014). *DECRETO 943.* Obtenido de Sitio de la Norma: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=59048

Modelo Nacional de Gestión de Riesgos de Seguridad Digital https://www.urnadecristal.gov.co/sites/default/files/MODELO%20DE%20GESTI%C3%93N%20DE%20RIESGOS%20DE%20SEGURIDAD%20DIGITAL.PDF

Gobierno de Colombia, Guía de orientación para la gestión de riesgos para la seguridad digital en el gobierno nacional territoriales y sector público.

Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia. Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia Primera Edición

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN, Política Nacional de Seguridad Digital en Colombia (2016).

Norma Técnica Colombiana NTC-ISO/IEC 27005:2009 TECNOLOGÍA DE LA INFORMACIÓN, TÉCNICAS DE SEGURIDAD, GESTIÓN DE RIESGOS EN LA SEGURIDAD D ELA INFORMACIÓN.

Norma Técnica Colombiana NTC-ISO/IEC 31000:2018 GESTION DEL RIESGO. PRINCIPIOS Y DIRECTRICES

Norma Técnica Colombiana UNE-ISO 31000:2018 GESTION DEL RIESGO. PRINCIPIOS Y DIRECTRICES

Norma Técnica Colombiana NTC-ISO 27001:2013 GESTION DE SEGURIDAD DE SISTEMAS DE INFORMACION. PRINCIPIOS Y DIRECTRICES

17. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción del cambio**
1	08-03-2017	Documento Original.
2	07-06-2018	Se modifica el documento de acuerdo con los lineamientos dictados por el DAFP a la administración de los riesgos por proceso y de corrupción.
3	27-03-2019	Se actualizó la normativa aplicable y el alcance donde se incluye Seguridad de la Información y Datos Personales, los tipos de riesgos que se van a controlar, los de seguridad de la información y de datos personales, así mismo se adjuntaron las etapas en la gestión del riesgo (riesgos digitales, de datos personales, de seguridad y privacidad de la información) y se adhirió Derechos de Autor. Finalmente se actualizó la Bibliografía y se realizaron ajustes de forma en la tabla de contenido.
4	24-08-2019	- Ajuste con base a la Versión 4 de la guía DAFP emitida en octubre de 2018. - Ajuste en Objetivo, Alcance, Política de administración del riesgo, Glosario, Tipos de riesgos que se van a controlar, Roles, responsabilidades, coordinación y articulación, Derechos de autor, Identificación y gestión del riesgo Riesgos por proceso), Identificación y gestión del riesgo Riesgos por Corrupción), Identificación y gestión del riesgo Riesgos por seguridad de la información, datos personales, seguridad y privacidad de la información), Seguimiento a los riesgos. -Inclusión de Administración de oportunidades -Ajuste de componentes de gestión de Seguridad de la Información
5	30/06/2020	Ajustes efectuados de los numerales de Riesgos por Procesos, Riesgos de Corrupción y Riesgos de Seguridad de la Información. Precisión de las zonas de calor para los Riesgos de Corrupción Se Ajusta el periodo de seguimiento de los Riesgos de Corrupción. Se ajusta el periodo de Evaluación de todas las tipologías de Riesgos. Se detalla dentro de la política el manejo de la información reservada y clasificada. Actualización de responsabilidades de la Primera Línea de Defensa
6	21/09/2021	Actualización integral de todos los numerales por la actualización de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública en su Versión 5 emitida en diciembre 30 de

		2020. Se Incluye la Ruta metodológica para la implementación del SARLAFT en las entidades distritales.
7	05/07/2022	Se ajusta el capítulo de Riesgos de Seguridad de la Información el cual se alineó con la Guía para la Gestión y Clasificación de Activos de Información del MINTIC, versión 1.0 del 15 de marzo del 2016.

	ELABORÓ	REVISÓ
NOMBRE	Pablo Molano Parra Diego Mauricio Usme González	Mary Buitrago Sierra Jorge Velasquez Perilla
CARGO	Contratista – OAP Contratista - TIC	Profesional Universitario – OAP Contratista – Enlace Operativo MIPG TIC
FIRMA