Firma de Autorizaciones		
Elaboró	**Revisó**	**Aprobó**
Contratista SIG Oficina Asesora de Planeación	**Jefe Oficina de Control Interno**	**Jefe Oficina Asesora de Planeación**

Control de Cambios	
Fecha	**Descripción**
Marzo de 2014	Elaboración del documento
Noviembre de 2017	Ajuste y actualización general del documento. Adicionalmente se ajusta de conformidad con la adopción de la política de administración del riesgo mediante Resolución 108 del 16 de noviembre de 2017
Marzo 2018	Se incluyen lineamientos de la Guía de Administración del riesgo 2014 del Departamento Administrativo de la Función Pública - DAFP y la Guía para la Gestión del Riesgo de Corrupción 2015 de la Secretaría de Transparencia de la Presidencia de la República.
Noviembre 2018	Se actualiza el documento de acuerdo con los nuevos lineamientos de la Guía de Administración del riesgo 2014 del Departamento Administrativo de la Función Pública – DAFP
Diciembre 2020	Se actualiza el documento con los lineamientos para el mapa de aseguramiento de la entidad, así como la actualización con base en la Guía de Administración del riesgo 2018 del Departamento Administrativo de la Función Pública – DAFP mejorando el seguimiento a los riesgos y controles definidos en el mapa de riesgos.
Diciembre 2021	Inclusión lineamientos Lavado de Activos y Financiación del Terrorismo y actualización a la versión 5 de la Guía de la Administración del Riesgo del DAFP.
Mayo 2023	Actualización general del instructivo de acuerdo con la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6. Dirección de Gestión y Desempeño Institucional noviembre 2022. Función Pública.
Agosto 2024	Se realizan ajustes al marco metodológico para la gestión del riesgo de acuerdo con los lineamientos vigentes y se optimizan los criterios del riesgo buscando un ejercicio acorde con el contexto de la Entidad. Adicional a esto, se incluyen elementos de Riesgos de Seguridad de la Información, Fiscales y de Lavado de Activos y Financiación de Terrorismo.

TABLA DE CONTENIDO

1. OBJETIVO

Definir el marco metodológico para la identificación, análisis, valoración y manejo de los riesgos asociados a los procesos del Instituto para la Investigación Educativa y el Desarrollo Pedagógico - IDEP, mediante la aplicación de herramientas actuales y aplicables a la gestión de la entidad, con el fin de aportar a la garantía del cumplimiento de los objetivos institucionales.

2. ALCANCE

El presente instrumento es aplicable a todos los procesos que hacen parte del modelo de operación de la entidad y considera su vinculación con los planes, programas y proyectos que se desarrollen y consideren pertinente su aplicación. Inicia desde la etapa de la identificación y finaliza con el monitoreo, evaluación independiente y la retroalimentación de los resultados a la primera línea de defensa y línea estratégica para la toma de decisiones. Incluye criterios de riesgos operacionales, de corrupción, de seguridad de la información, fiscales y aquellos asociados con lavado de activos y financiación de terrorismo.

3. REFERENCIAS NORMATIVAS

- **Ley 87 de 1993** Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

- **Ley 489 de 1998:** Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.

- **Ley 1474 de 2011:** Estatuto Anticorrupción. Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.

- **Ley 599 de 2000 (Código Penal Colombiano):** contempla otras actuaciones prohibidas generadoras de recursos ilícitos

- **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.

- **CONPES 01 de 2019:** Política Pública de Transparencia, Integridad y No Tolerancia con la Corrupción.

4. DEFINICIONES

A continuación, se presentan algunas definiciones aplicables para la documentación y la actualización del Sistema de Gestión del Instituto para la Investigación Educativa y el Desarrollo Pedagógico - IDEP, para las que no se encuentren dentro de este documento, aplican las definiciones establecidas en la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública (DAFP).

Aceptar el riesgo: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular después de realizar un análisis y considerar los niveles de riesgo.

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

Administración de Riesgos: Es el proceso continuo basado en el conocimiento, evaluación y manejo de los riesgos que mejora la toma de decisiones organizacionales.

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

Análisis de riesgo: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias**.**

Apetito del 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.

Aseguramiento: Es un examen objetivo de evidencias con el propósito de obtener una evaluación independiente de los procesos de gestión, de riesgos, control y gobierno de una organización.

Autoevaluación: Elemento de control que, basado en un conjunto de mecanismos de verificación y evaluación, determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.

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.

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

Compartir el riesgo: Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

Control: Medida que permite reducir o mitigar un riesgo.

Control automático: Son ejecutados por un sistema

Control correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos

Control detectivo: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control manual: Controles que son ejecutados por personas.

Control preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

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.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado o particular.

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 ex- presa 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 una entidad.

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.

Frecuencia: Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Gestión del riesgo de corrupción: Es el conjunto de actividades coordinadas para dirigir y controlar una organización con respecto al riesgo de corrupción.

Identificación del riesgo: Elemento cuyo objetivo es identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos.

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.

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 aseguramiento: Herramienta diseñada con el fin de establecer una adecuada coordinación de los diferentes actores internos y externos relacionados con la función de aseguramiento en una organización, y de esta forma minimizar la duplicidad de esfuerzos y dar una cobertura adecuada a las diferentes tareas relacionadas con el riesgo, control y auditoría.

Monitorear: Comprobar, Supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles 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 poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Oficial de Cumplimiento: Es la persona responsable del cumplimiento del sistema anti lavado de activos y financiación del terrorismo.

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.

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

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Proceso de administración de riesgo: Aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la administración del riesgo.

Reducción del riesgo: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.

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. 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 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 di- rectamente 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

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.

Sistema de Administración de Riesgo: Conjunto de elementos del direccionamiento estratégico de una entidad concerniente a la Administración del Riesgo.

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.

5. METODOLOGÍA

5.1. Conocimiento de la Entidad

Es indispensable conocer a profundidad la entidad y sus elementos estratégicos para identificar el escenario de riesgo al que está expuesta.

Para la aplicación de la política de la gestión de riesgos se parte de la revisión inicial de los siguientes elementos:

- Misión.
- Visión.
- Objetivos estratégicos.
- Mapa de procesos y su caracterización.
- Estructura funcional.
- Planes, programas y proyectos priorizados por la administración.

Esta información está disponible en la página web de la entidad.

5.2 Institucionalidad

El Modelo Integrado de Planeación y Gestión (MIPG) define para su para su operación articulada la creación del Comité Institucional de Gestión y Desempeño (CIGD), regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno (CICCI), reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de

2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Instancia	Rol
Comité Institucional de Gestión y Desempeño (CIGD)	Instancia en la que se analiza la gestión del riesgo y se aplican las mejoras
Comité Institucional de Coordinación de Control Interno (CICCI)	Instancia que aprueba el marco de referencia de la gestión del riesgo y se le presenta el análisis de eventos y riesgos críticos.
Líderes de Proceso	Responsables de gestionar los riesgos y hacer seguimiento en 1a. línea.
Oficina Asesora de Planeación (2a. Línea de Defensa)	Capacita, acompaña metodológicamente, genera recomendaciones, define metodología.
Servidores y Contratistas	Responsables de aplicar los controles en el día a día.

Tabla 1. Operatividad; Institucionalidad para la gestión del Riesgo.

5.3 Desarrollo Metodológico:

La línea metodológica para la gestión del riesgo en el IDEP se desarrolla basada en la estructura planteada por el estándar internacional ISO 310000 en articulación con la Guía para la administración del riesgo y el diseño de controles en las entidades públicas del Departamento Administrativo de la Función Pública, en sus versiones más recientes.

Figura 1. Ciclo de administración de riesgos, basado en ISO 31000

La metodología planteada por el DAFP requiere de un análisis inicial de la gestión en la entidad desde un punto de vista estratégico y desglosa la aplicación de tres (3) pasos para su desarrollo. Adicionalmente vincula el reconocimiento de escenarios de riesgo desde la perspectiva de corrupción y de seguridad de la información.

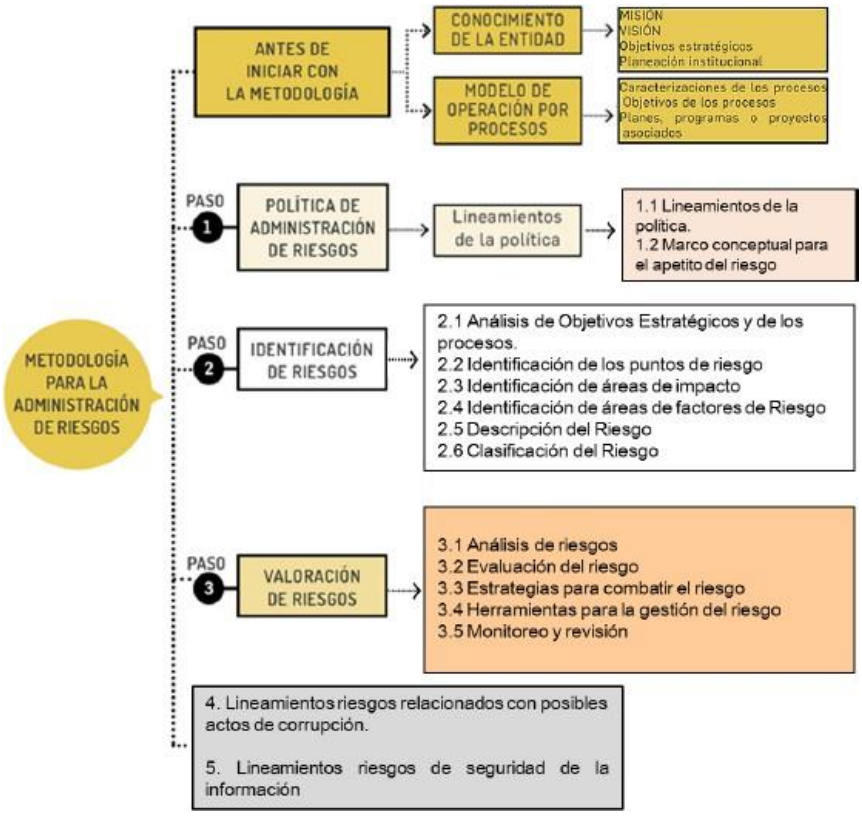


Figura 2 Metodología para la administración del riesgo, Departamento Administrativo de la Función Pública, 2020.

5.3.1 Política de Administración del Riesgo

La Política de Administración del Riesgo adoptada por el IDEP es definida por la Alta Dirección bajo el liderazgo de la Dirección y es presentada para su aprobación ante el Comité Institucional de Coordinación de Control Interno (CICCI).

Se desarrolla a través de este instrumento documentado, dónde se definen las etapas de administración de riesgos, la periodicidad para el monitoreo y los niveles de responsabilidad sobre la gestión de los riesgos en el marco de los roles de las líneas de defensa.

Implica el compromiso institucional frente a la gestión del riesgo, desde la identificación, análisis, valoración de sus riesgos hasta el tratamiento efectivo que permita prevenir o mitigar la materialización de los riesgos, realizar seguimiento e implementar acciones de

mejora para evitar que se afecte el normal desarrollo de los procesos y se logre el cumplimiento de los objetivos institucionales.

El marco metodológico de la Gestión del Riesgo en el IDEP considerará las siguientes categorías para su "tratamiento", entendido como la respuesta establecida por la primera línea de defensa para el manejo de los diferentes riesgos. Los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. El tratamiento o respuesta dado al riesgo, se enmarca en las siguientes categorías

Categoría	Tratamiento riesgo
Aceptar el riesgo	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).
Reducir el riesgo	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
Evitar el riesgo	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
Compartir el riesgo	Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

Tabla 2: Categorías tratamiento del riesgo, Guía para la Administración del Riesgo - DAFP.

La determinación de las acciones para el tratamiento del riesgo parte de la valoración de los mismos, en las que se encuentra las siguientes categorías:

Bajo	Nivel de riesgo en el que la probabilidad de ocurrencia, o el impacto que podría generar la materialización del riesgo es baja y no afecta el logro de los objetivos. Es en este nivel donde se establece el **"Apetito del riesgo del IDEP"**.
Moderado	Nivel de riesgo en el que la conjugación de la probabilidad y el impacto pueden llegar a generar desviaciones al cumplimiento de los objetivos en caso de materializarse el riesgo. En este nivel se establece la **"Tolerancia del riesgo del IDEP"**, entendido como el valor de la máxima desviación admisible del nivel de riesgo con respecto al apetito de riesgo.
Alto	Es la valoración del riesgo en la cual se determinan acciones para el manejo prioritario de los riegos, pues de no hacerlo, podrían verse seriamente comprometidos el logro de los objetivos y la continuidad de la operación.
Extremo	Es el valor máximo de combinación de los criterios de impacto y frecuencia que puede generar efectos catastróficos frente al cumplimiento de los objetivos planteados. Es la medida máxima de **"Capacidad de riesgo"** entendida como el máximo valor del nivel de riesgo que la entidad puede soportar.

Tabla 3: Niveles del riesgo. Elaboración propia.

A partir de estas valoraciones, se establecen las siguientes premisas para el tratamiento de los riesgos:

- Cuando el nivel del riesgo residual quede en nivel de riesgo **"bajo"**, cada líder o responsable del correspondiente proceso podrá **aceptar** el riesgo, sin embargo, en conjunto con sus equipos pueden establecer acciones adicionales a los controles establecidos que permitan mantener o reducir la probabilidad de ocurrencia del riesgo.

- Cuando el nivel del riesgo residual quede en zona de riesgo **"moderado"**, cada líder o responsable del correspondiente proceso en conjunto con sus equipos, deberán establecer acciones o controles adicionales a los establecidos que permitan **reducir** la probabilidad de ocurrencia del riesgo o su impacto.

- Cuando el nivel del riesgo residual quede en la zona de riesgo **"alta"** o **"Extrema"**, cada líder o responsable del correspondiente proceso en conjunto con sus equipos, deberán establecer acciones o controles adicionales a los establecidos que permitan **evitar, reducir, compartir o transferir** el riesgo.

- Los **riesgos de corrupción** son inaceptables e intolerables y bajo ninguna circunstancia se pueden asumir, de tal forma que se implementarán controles preventivos y acciones encaminadas a tratar este tipo de riesgo y sus consecuencias.

5.3.2 Identificación del Riesgo

Esta etapa tiene como objetivo identificar los riesgos asociados a los procesos. Para ello se debe tener en cuenta el contexto en el que opera la entidad analizando los factores externos (políticos, económicos, sociales, tecnológicos, ambientales, legales) y los factores internos (debilidades, fortalezas) que incidan en el cumplimiento de los objetivos. Adicional a esto, se debe considerar la caracterización de cada proceso incluyendo su objetivo y alcance y los factores internos y externos que pueden afectar el cumplimiento de los objetivos.

5.3.2.1 Identificación de recursos

Dentro de la gestión de los riesgos de cada proceso se cuentan con recursos que permiten evitar y mitigar los riesgos identificados. Estos recursos son:

- Recursos humanos.

Se refiere al personal destinado a la aplicación de los controles, monitoreo de los riesgos y reporte de su seguimiento. Se debe reportar los cargos que correspondan como profesional especializado, jefe de la dependencia, contratista, entre otros.

- Recursos técnicos.

Se refiere a las herramientas con las que cuenta el proceso para la mitigación de los riesgos. Se deben reportar herramientas como aplicativos, programas, equipos de control, entre otros.

- Recursos físicos y/o de infraestructura.

Se refiere a los medios con los cuales se realiza la gestión de los riesgos. Se deben reportar los recursos con los que se cuenta como equipos de cómputo, oficinas, maquinaría, entre otros.

5.3.2.2 Análisis de objetivos estratégicos y de los procesos:

Consiste en el análisis de los objetivos estratégicos garantizando su alineación con la misión y la visión institucional y su despliegue desde los procesos y su estructura.

5.3.2.3 Identificación de los puntos de riesgo

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

5.3.2.4 Identificación de áreas de impacto

Consiste en la definición de la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

5.3.2.5 Identificación de áreas de factores de riesgo

Consiste en la identificación de las fuentes generadoras de riesgos:

Factor de riesgo	**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
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)

Factor de riesgo	**Definición**	**Descripción**
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

Tabla 4: Categorías tratamiento del riesgo. Fuente: Guía para la Administración del Riesgo – DAFP

5.3.2.6 Descripción del riesgo:

Consiste en la documentación del riesgo que debe contener todos los detalles que sean necesarios y de fácil entendimiento, tanto para el líder del proceso, como para personas externas. De acuerdo con los lineamientos del DAFP, la siguiente estructura facilita su redacción y claridad, iniciando con la frase “posibilidad de” y se analizan los siguientes aspectos:

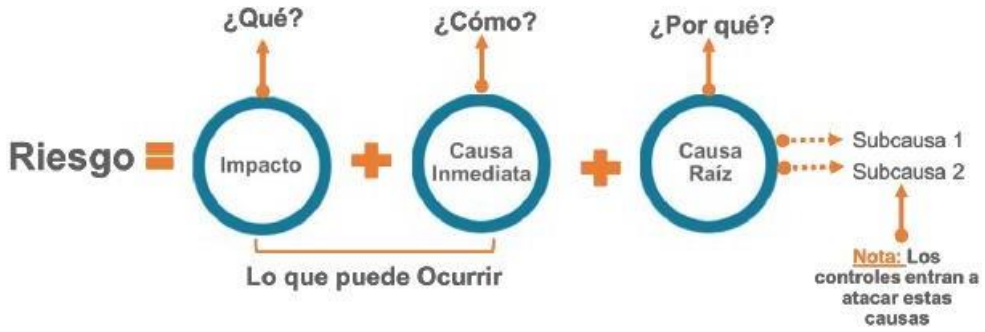


Figura 3: Descripción del Riesgo – Fuente DAFP

En la redacción del riesgo es importante considerar:

- 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. En otras palabras, pueden existir riesgos que tengan una naturaleza similar pero su redacción debe aterrizarse a la particularidad del proceso en el cual se identifican. Ejemplo: pérdida de expedientes.

5.3.2.7 Clasificación del riesgo

Consiste en agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías.

Clasificación del riesgo	Descripción	Factores de Riesgo
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	Procesos
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	Evento Externo
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales 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.	Talento Humano
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.	Tecnología
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.	Varios Factores Asociados
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.	Infraestructura Evento Externo

Tabla 5: Categorías Clasificación del riesgo. Fuente: Guía para la Administración del Riesgo – DAFP

5.3.3 Valoración del Riesgo

Comprende las fases de análisis, evaluación y tratamiento del riesgo. Incluye las herramientas para la gestión del riesgo, monitoreo y revisión. Se desarrolla a partir de la identificación de la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

5.3.3.1 Análisis del riesgo

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

Probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo. Está asociada a la exposición al riesgo de la actividad que se esté analizando. De este modo, la probabilidad inherente será calculada con respecto a la frecuencia del desarrollo de la actividad realizada y la posibilidad de la ocurrencia del evento**.** En la tabla siguiente se establecen los criterios que definen el nivel de probabilidad del IDEP.

Nivel	Probabilidad	Descripción
5	**Muy Alta**	La actividad asociada con el riesgo se desarrolla con una alta frecuencia y la posibilidad de ocurrencia del evento analizado es alta.
4	**Alta**	La actividad asociada con el riesgo se desarrolla con una alta frecuencia y la posibilidad de ocurrencia del evento analizado presenta un nivel medio.
3	**Media**	La actividad que conlleva el riesgo se ejecuta con una frecuencia moderada y la posibilidad de ocurrencia del evento analizado presenta un nivel medio.
2	**Baja**	La actividad asociada con el riesgo se realiza en una baja frecuencia y dadas las condiciones de operación, la posibilidad de ocurrencia del evento analizado presenta un nivel medio.
1	**Muy Baja**	La actividad que conlleva el riesgo se ejecuta rara vez y dadas las condiciones de operación, la posibilidad de ocurrencia del evento presenta un nivel bajo.

Tabla 6: Calificación de probabilidad. Fuente: Guía de administración del riesgo DAFP.

Para la definición objetiva de la probabilidad se cuenta con las siguientes subdivisiones del criterio de forma que se facilite emitir un juicio a la cuantificación de la ocurrencia del evento:

Ocurrencia	Frecuencia	Condiciones	Trazabilidad	Vr
No ha ocurrido en la entidad.	La actividad desarrollada que posibilita la materialización del riesgo tiene una frecuencia de ejecución Anual.	Las condiciones actuales hacen que la materialización del riesgo sea un evento improbable.	Se cuenta con registros históricos que permitan llevar la trazabilidad de la ocurrencia de eventos relacionados.	1
Ha ocurrido una vez en los últimos cinco años en la Entidad.	La actividad desarrollada que posibilita la materialización del riesgo tiene una frecuencia de ejecución semestral.	Las condiciones actuales hacen que la materialización del riesgo sea un evento con una baja probabilidad de ocurrencia.	Se cuenta con registros históricos que posibilitan el análisis de situaciones similares y que permitan analizar eventos similares.	2

Ocurrencia	Frecuencia	Condiciones	Trazabilidad	Vr
Ha ocurrido una vez en los últimos dos años en la Entidad.	La actividad desarrollada que posibilita la materialización del riesgo tiene una frecuencia de ejecución mensual.	Las condiciones actuales hacen que la materialización del riesgo sea un evento con una probabilidad moderada.	Existen datos que pueden brindar información frente a la ocurrencia de un evento, pero esta información debe ser reconstruida.	3
Ha ocurrido una vez en la Entidad en el último año.	La actividad desarrollada que posibilita la materialización del riesgo tiene una frecuencia de ejecución semanal.	Las condiciones actuales hacen que la materialización del riesgo sea un evento con una alta probabilidad de ocurrencia.	Existen algunos registros de información relacionada, pero estos datos no están inmediatamente disponibles.	4
Ha ocurrido más de una vez en la entidad en el último año.	La actividad desarrollada que posibilita la materialización del riesgo tiene una frecuencia de ejecución diaria.	Las condiciones actuales hacen que la materialización del riesgo sea un evento casi certero.	No se cuenta con registros históricos que permitan llevar la trazabilidad de la ocurrencia de eventos relacionados.	5

Tabla 7: Subcriterios de probabilidad. Fuente: Elaboración propia.

El evaluador debe seleccionar una opción para cada criterio, de forma que finalmente se promedien las valoraciones y se emita un nivel de probabilidad con menor sesgo.

Impacto

Se entiende como impacto las afectaciones económicas y reputacionales a las que se puede llegar por la materialización de un evento.

Cuando se identifique simultáneamente un impacto económico y reputacional en el análisis de un riesgo con diferentes niveles para cada uno, en la valoración se debe tomar el nivel más alto de los dos, por ejemplo: para un riesgo se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el nivel más alto de los dos, que en este caso sería el nivel moderado.

Bajo este esquema se facilita el análisis para quien desarrolla el ejercicio, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Costo	Tiempo	Alcance	Operatividad	Vr
La materialización del riesgo no conlleva a pérdidas económicas.	En caso de materializarse el riesgo afectaría los tiempos de operación en periodos inferiores a cuatro horas.	El riesgo tiene una afectación puntual en el procedimiento, no afecta otras tareas desarrolladas en el proceso evaluado.	La materialización del riesgo afectaría levemente la operación normal del proceso.	1
La materialización del riesgo conlleva a pérdidas económicas mínimas que para su atención no requieren modificaciones en términos presupuestales	En caso de materializarse el riesgo afectaría los tiempos de operación entre uno y dos días.	El riesgo tiene una afectación en el procedimiento y afecta algunos procedimientos del proceso evaluado.	La materialización del riesgo afectaría la operación normal del proceso.	2

Costo	Tiempo	Alcance	Operatividad	Vr
La materialización del riesgo conlleva a pérdidas económicas mínimas que implican modificaciones leves a los presupuestos de los proyectos de inversión relacionados.	En caso de materializarse el riesgo afectaría los tiempos de operación en más de dos y hasta tres días.	El riesgo tiene una afectación local y tiene impacto sobre el proceso evaluado.	La materialización del riesgo afectaría la operación normal del proceso e implica el despliegue de una contingencia	3
La materialización del riesgo conlleva a pérdidas económicas considerables y modifica los presupuestos del o de los proyectos de inversión con que tenga relación.	En caso de materializarse el riesgo afectaría los tiempos de operación en más de tres y hasta cuatro días.	El riesgo tiene una afectación extensa y afecta otro proceso además del proceso evaluado.	La materialización del riesgo afectaría la operación normal del proceso, desplazando varios recursos para su atención.	4
La materialización del riesgo conlleva a pérdidas económicas significativas que afectan directamente el cumplimiento de los objetivos del o de los proyectos de inversión con que tenga relación.	En caso de materializarse el riesgo afectaría los tiempos de operación en periodos superiores a cuatro días.	El riesgo tiene una afectación extensa y afecta varios procesos además del proceso evaluado.	La materialización del riesgo afectaría por completo la operación normal del proceso.	5

Tabla 8: Subcriterios de impacto. Fuente: Elaboración propia.

El evaluador debe seleccionar una opción para cada criterio, de forma que finalmente se promedien las valoraciones y se emita un nivel de impacto con menor con menor sesgo.

Para guardar coherencia con las guías establecidas actualmente, la valoración final del impacto responderá a los criterios planteados por el DAFP en la siguiente matriz:

Nivel	Impacto	Afectación económica	Descripción
5	**Catastrófico**	Mayor a 100 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.
4	**Mayor**	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
3	**Moderado**	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
2	**Menor**	Entre 5 y 10 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
1	**Leve**	Afectación menor a 5 SMLMV	El riesgo afecta la imagen de algún área de la organización.

Tabla 9: Calificación de impacto a partir del planteamiento de la Guía de administración del riesgo DAFP.

Cabe aclarar que, para la valoración de riesgos asociados con corrupción, ningún impacto puede estar ranqueado en los niveles “menor” o “leve”.

Evaluación de Riesgos

Consiste en el análisis del cruce de la probabilidad de ocurrencia del riesgo y su impacto, se busca determinar la zona de riesgo en un escenario inicial (riesgo inherente).

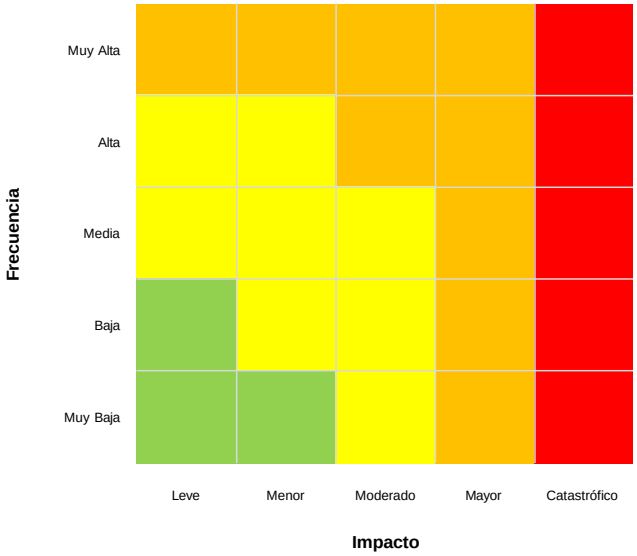


Figura 4: Mapa de calor a partir del planteamiento de la Guía de administración del riesgo DAFP.

De acuerdo con la calificación de probabilidad y de impacto definidas, se procede a determinar la zona de riesgo inherente.

Bajo	Nivel de riesgo en el que cada líder o responsable del proceso podrá aceptar el riesgo, sin embargo, pueden establecer acciones adicionales a los controles establecidos que permitan mantener o reducir la probabilidad de ocurrencia del riesgo.
Moderado	Nivel de riesgo en el que el líder o responsable del proceso, en conjunto con su equipo, debe establecer acciones o controles adicionales a los actualmente planteados, de forma que se reduzca la probabilidad de ocurrencia del riesgo o su impacto.
Alto	Es la valoración del riesgo en la que cada líder o responsable del correspondiente proceso en conjunto con sus equipos, deberán establecer acciones que permitan evitar, reducir, compartir o transferir el riesgo.
Extremo	Es el valor máximo de combinación de los criterios de impacto y frecuencia que puede generar efectos catastróficos frente al cumplimiento de los objetivos planteados, por lo anterior, los riesgos ubicados en este nivel de riesgo deberán documentar acciones prioritarias y realizar un seguimiento exhaustivo y en los casos en que un riesgo esté valorado en impacto “catastrófico” requerirá del desarrollo de un plan de contingencia.

Tabla 10. Valoración de riesgo Inherente.

5.3.3.1 Identificación de Controles

Estructura para la descripción del control

Una vez establecido el nivel de riesgo inherente se deben identificar los controles, entendidos como, los instrumentos que permitirán reducir o mitigar el riesgo, teniendo en cuenta lo siguiente:

- La identificación de los controles se realiza por medio de entrevistas con los líderes de procesos o servidores expertos en su quehacer, aplicando el criterio de experto.
- Un mismo control puede servir para atacar una o varias causas dentro de un mismo riesgo.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Los controles están orientados a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

Para la redacción de los controles se debe considerar la siguiente estructura:

Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

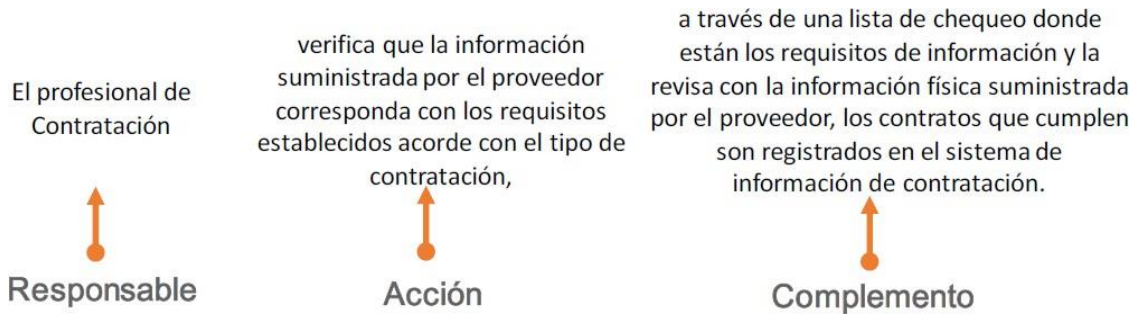


Figura 5: Estructura del control tomado del DAFP.

Adicional a lo anterior, se recomienda que en el diseño de controles se consideren los siguientes criterios:

Criterio	Descripción
Objetivos	Un control debe responder a un propósito y no depender del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener.
Viables	Los controles deben estar alineados a la normatividad vigente y deben ser viables económicamente en contexto con la realidad de la entidad.
Pertinentes	Los controles están orientados específicamente a atacar las causas o consecuencias que posibilitan la desviación de los objetivos.
Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de aplicar.
Medibles	Este criterio resalta la importancia del establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad.
Periódicos	Para cada control se debe definir la frecuencia de aplicación.
Efectivos	Eliminan o mitigan las causas o consecuencias y aportan al logro de los objetivos, evitando la materialización de los riesgos.
Asignables	Tienen responsables definidos para su ejecución.

Tabla 11: Criterios para el diseño de los controles; Elaboración propia

Atributos para el Diseño de Control

De acuerdo con la naturaleza del control, los controles pueden ser de tipo preventivo o detectivo si atacan las causas del riesgo por lo que disminuyen su probabilidad de ocurrencia, o correctivos si atacan las consecuencias del riesgo por lo que buscan reducir el impacto en caso de materialización.

Una vez identificados los controles se deben tener en cuenta los atributos para el diseño del control: se tienen atributos de eficiencia (los cuales se califican e inciden en la valoración del nivel de riesgo residual) y atributos informativos (no tienen incidencia en la efectividad su fin es conocer el entorno del control).

Atributo	Criterio	Pond	Descripción	Descripción	Peso
Atributos de Eficiencia	Tipo	30%	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	30%
			Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	20%
			Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%

Atributo	Criterio	Pond	Descripción	Descripción	Peso
	Implementación	10%	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	20%
			Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	10%
Atributos Informativos	Documentación	20%	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	20%
			Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	0%
	Frecuencia	30%	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	30%
			Esporádica	El control se aplica algunas veces cuando se realiza la actividad que conlleva el riesgo.	20%
			Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	10%
	Evidencia	10%	Con registro	El control deja un registro permite evidencia la ejecución del control.	10%
			Sin registro	El control no deja registro de la ejecución del control.	0%

Tabla 12: Atributos y valoración de un control

En aquellos casos en donde se identifique que un control no se encuentra documentado (atributo de “Documentación”), el lider de proceso debe formular la documentación como accion de manejo en aras de formalizar el control en los documentos publicados en el SIG.

De acuerdo con el tipo de control se puede dar el desplazamiento en la matriz de calor.

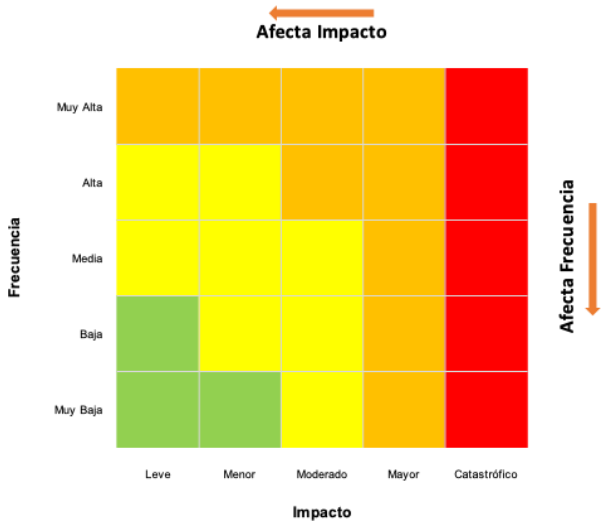


Figura 6: Afectación del control tomado del DAFP.

La información de valoración de los controles y su posterior afectación frente al riesgo Inherente se debe diligenciar en el formato FT-MIC-03-07 Mapa de riesgos de gestión.

5.3.3.2 Evaluación de los controles

Para evaluar los controles establecidos se tienen en cuenta los criterios establecidos en el apartado “Atributos para el Diseño de Control” con su respectiva ponderación. Tras la selección de estos criterios de valoración, el control se evaluará como débil, moderado o fuerte siendo los controles débiles los que no aportan a la disminución del nivel de riesgo inherente, en cuyo caso el nivel de riesgo residual será equivalente al inherente. Los controles moderados pueden disminuir en un nivel el criterio del riesgo, dependiendo de la afectación de control (Frecuencia, impacto o frecuencia e impacto). Finalmente, los controles fuertes pueden disminuir en dos niveles el criterio del riesgo, dependiendo de la afectación de control (Frecuencia, impacto o frecuencia e impacto).

Esta valoración tendrá impacto en la valoración final de los riesgos, mediante la identificación del nivel de riesgo residual.

5.3.3.3 Nivel de Riesgo Residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el

siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Cuando la solidez individual del control es ***fuerte***, no es necesario que las acciones esten direccionadas al fortalecimiento del control. En todos los demás casos es factible formular dichas acciones de tratamiento.

5.3.4. Manejo del Riesgo

Hace referencia a la decisión que se toma frente al nivel de riesgo residual obtenido, teniendo como opciones de tratamiento aceptar, reducir, evitar o compartir el riesgo, considerando lo establecido en la Política de la Administración del Riesgo del IDEP, reiterando que las acciones para el tratamiento del riesgo parten de la valoración de los mismos, como se establece a continuación:

- Cuando el nivel del riesgo residual quede en nivel de riesgo **"bajo"**, cada líder o responsable del correspondiente proceso podrá **aceptar** el riesgo, sin embargo, en conjunto con sus equipos pueden establecer acciones adicionales a los controles establecidos que permitan mantener o reducir la probabilidad de ocurrencia del riesgo.

- Cuando el nivel del riesgo residual quede en zona de riesgo **"moderado"**, cada líder o responsable del correspondiente proceso en conjunto con sus equipos, deberán establecer acciones o controles adicionales a los establecidos que permitan **reducir** la probabilidad de ocurrencia del riesgo o su impacto.

- Cuando el nivel del riesgo residual quede en la zona de riesgo **"alta"** o **"Extrema"**, cada líder o responsable del correspondiente proceso en conjunto con sus equipos, deberán establecer acciones o controles adicionales a los establecidos que permitan **evitar, reducir, compartir o transferir** el riesgo.

Para cada una de las actividades que conforman el plan de acción se debe especificar el responsable, plazo de ejecución, y el entregable o medio de verificación. Definiendo el indicador correspondiente para determinar el avance del plan de acción.

Cuando en la ejecución de un plan se requiera de la participación de otras áreas, el Líder o responsable de proceso debe concertar con el área involucrada su participación para la formulación del plan.

Los planes de acción pueden comprender acciones enfocadas a prevenir que el riesgo ocurra actuando sobre las causas del riesgo (afectando la probabilidad), o acciones que mitiguen el impacto de sus consecuencias en caso de materialización.

En la formulación de los planes de acción se podrían considerar actividades relativas a revisar los controles que requieran mejorarse o fortalecerse, el diseño e implementación de nuevos controles considerando en todo caso la relación costo beneficio (optimización o

adopción de nuevas prácticas o herramientas), actividades que permitan incidir sobre los factores del riesgo, actividades que permitan transferir o compartir el riesgo.

En todo caso los líderes y responsables de proceso encargados de gestionar el riesgo deben velar porque los controles se encuentren documentados dentro del SIG.

Al cierre del plan de acción se debe revisar si alguna de las actividades planteadas obedece a algún control nuevo que deba relacionarse al riesgo, si modifica los atributos de algún control, o si el plan tiene algún efecto sobre la valoración del riesgo.

5.3.5. Monitoreo y Revisión

Las actividades de monitoreo y revisión se aplican en todas las etapas de la gestión de riesgos e incluye la planificación, recopilación y análisis de la información, registrando los resultados y brindando la respectiva retroalimentación. Permiten identificar el adecuado diseño de los controles y su correcto funcionamiento, y en los casos que aplique, mejorar o definir nuevos controles, obtener información adicional que permita mejorar la valoración del riesgo, sacar provecho de las lecciones aprendidas, detectar posibles cambios en el contexto interno o externo, identificar posibles riesgos emergentes y evaluar su inclusión en el mapa de riesgos, así como identificar si se requiere modificar o actualizar los riesgos evaluados.

Se deben analizar los resultados derivados de la gestión del riesgo, partiendo de las matrices de riesgos y herramientas de gestión anteriormente mencionadas. En términos generales para el monitoreo de los riesgos se establece una periodicidad trimestral.

Como parte de la metodología, se establece que, para realizar el monitoreo y revisión de los riesgos, se implementó el uso compartido del Mapa de riesgos en la herramienta de que determine la Oficina Asesora de Planeación, en el cual las personas responsables del monitoreo y seguimiento ingresarán y diligenciarán los campos requeridos de acuerdo con las instrucciones que para ello imparta la Oficina Asesora de Planeación a través de correo electrónico y/o memorando.

5.3.6. Comunicación y Consulta

La consolidación del Mapa de riesgos le corresponde realizarla a la Oficina Asesora de Planeación, quien servirá de facilitador en el proceso de Gestión de Riesgos con las dependencias. La Comunicación y consulta se surtirá en todas las etapas de construcción del Mapa de riesgos. Concluido este proceso de participación deberá procederse a su divulgación Asegurándose que sea conocido por toda la Entidad.

5.3.6.1. Que hacer en caso de materialización de un riesgo

- El responsable del proceso debe reunirse con su equipo de trabajo para formular la(s) acción(es) correctiva(s) e incluirlas en el Plan de mejoramiento del proceso para mitigar las causas y consecuencias del riesgo identificadas. Esta reunión debe realizarse de manera inmediata una vez materializado el riesgo.

- El proceso debe enviar las acciones formuladas a la Oficina Asesora de Planeación para revisión metodológica, en un periodo que no supere los 5 días hábiles siguientes a la materialización del riesgo.
- El Plan de mejoramiento del proceso debe quedar actualizado y publicado en un periodo que no supere los 8 días hábiles siguientes a la materialización del riesgo.

5.3.6.2. Seguimiento a los riesgos

El seguimiento al mapa de riesgos por parte de los líderes de proceso debe realizarse cuatrimestralmente, de la siguiente manera:

Cuatrimestre	Reporte
Enero - Abril	Primera semana de Mayo
Mayo - Agosto	Primera semana de Septiembre
Septiembre - Diciembre	Mediados de Diciembre o según directriz del Comité Institucional de Gestión y Desempeño

Tabla 13: Seguimiento Mapa de riesgos del IDEP

El/la Jefe de Control Interno o quien haga sus veces, será responsable de verificar y evaluar la elaboración, visibilización, seguimiento y control del Mapa de Riesgos.

Este seguimiento a la Gestión del Riesgo se divide en dos etapas, la primera obedece al seguimiento a los ***riesgos institucionales***, para lo cual la Oficina de Control Interno podrá realizarlo de acuerdo con el Plan anual de auditoría, que ejecuta a los procesos de la entidad durante la vigencia. La segunda etapa corresponde al seguimiento a los ***riesgos de corrupción*** como parte de la Estrategia anticorrupción y de atención al ciudadano, para lo cual se realizará de igual manera tres (3) veces al año en las mismas fechas de seguimiento descritas anteriormente.

5.4. Lineamientos para la Gestión de Riesgos de Corrupción

Para la identificación de los riesgos de corrupción se aplican las mismas etapas de la gestión de riesgos mencionadas previamente, por lo que el formato a utilizar y los plazos para su reporte y seguimiento corresponden a los previamente descritos y en este numeral se enfatizará en las variaciones que aplican para el manejo de los riesgos de corrupción.

5.4.1 Definición del riesgo de corrupción

Independiente de la tipología la descripción del riesgo debe ser lo suficientemente clara sin dar lugar a ambigüedades tanto para el líder del proceso como para personas ajenas al proceso. El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Para la redacción de los riesgos de corrupción se debe tener en cuenta que deben concurrir los siguientes componentes:

Figura 7: Definición de un riesgo de corrupción

A continuación, se presentan los ejemplos de la aplicación de la estructura propuesta:

Acción u omisión	Uso del poder	Desviación de la gestión de lo público	Beneficio de un privado o un particular
Posibilidad de recibir o solicitar cualquier dadiva	para direccionar o modificar	un proceso de selección	para el beneficio de un tercero o de un particular.
Posibilidad de alterar información	de estados financieros de la entidad	para ocultar gestión indebida de los recursos	para el beneficio de un particular.
Posibilidad de recibir o solicitar cualquier dadiva	para manipular, alterar, modificar o proferir	fallos y certificaciones	para el beneficio de un particular.
Elaboración de estudios previos	modificados o alterados	estableciendo necesidades inexistentes o aspectos específicos	para el beneficio de un particular.

Tabla 14: Ejemplos riesgos de corrupción

5.4.2. Clasificación del Riesgo

La clasificación de los riesgos de corrupción toma en cuenta los mismos criterios utilizados para los riesgos de gestión.

5.4.3. Valoración del Riesgo de Corrupción

Al igual que los riesgos de operacionales, los riesgos de corrupción deben ser valorados en cuanto a probabilidad y a impacto. La probabilidad será valorada bajo los mismos criterios que los riesgos de gestión.

Con respecto a la valoración de los criterios de impacto, para los riesgos de corrupción solo se conciben tres niveles: Moderado, Mayor y Catastrófico, de acuerdo a lo establecido en la siguiente tabla:

NIVEL	DESCRIPTOR	DESCRIPCIÓN
20	Catastrófico	Afectación parcial al proceso y a la dependencia. Genera a medianas consecuencias para la entidad.
10	Mayor	Impacto negativo de la Entidad. Genera altas consecuencias para la entidad.
5	Moderado	Afectación parcial al proceso y a la dependencia. Genera medianas consecuencias para la entidad.

Tabla 15: Calificación del impacto riesgos de corrupción. Fuente: Guía para la Administración del Riesgo - DAFP.

Para determinar si el impacto es Catastrófico, Mayor o Moderado, se deben responder 19 preguntas referentes al riesgo identificado.

- ¿Afectar al grupo de funcionarios del proceso?
- ¿Afectar el cumplimiento de metas y objetivos de la dependencia?
- ¿Afectar el cumplimiento de misión de la entidad?
- ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?
- ¿Generar pérdida de confianza de la entidad, afectando su reputación?
- ¿Generar pérdida de recursos económicos?
- ¿Afectar la generación de los productos o la prestación de servicios?
- ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?
- ¿Generar pérdida de información de la entidad?
- ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?
- ¿Dar lugar a procesos sancionatorios?
- ¿Dar lugar a procesos disciplinarios?
- ¿Dar lugar a procesos fiscales?
- ¿Dar lugar a procesos penales?
- ¿Generar pérdida de credibilidad del sector?
- ¿Ocasionar lesiones físicas o pérdida de vidas humanas? (Si esta respuesta es Afirmativa, el riesgo se considera como Catastrófico)
- ¿Afectar la imagen regional?
- ¿Afectar la imagen nacional?
- ¿Genera daño Ambiental?

Estas preguntas se contestan afirmativa o negativamente (si o no) calculando el número de respuestas afirmativas a las 19 preguntas formuladas. De acuerdo con esto se define el nivel de impacto de la siguiente manera:

- 1 a 5 = Moderado
- 6 a 11 = Mayor
- 12 a 19 = Catastrófico

El nivel de riesgo inherente de corrupción es determinado a partir del cruce de la valoración de los anteriores criterios en el siguiente mapa de calor:

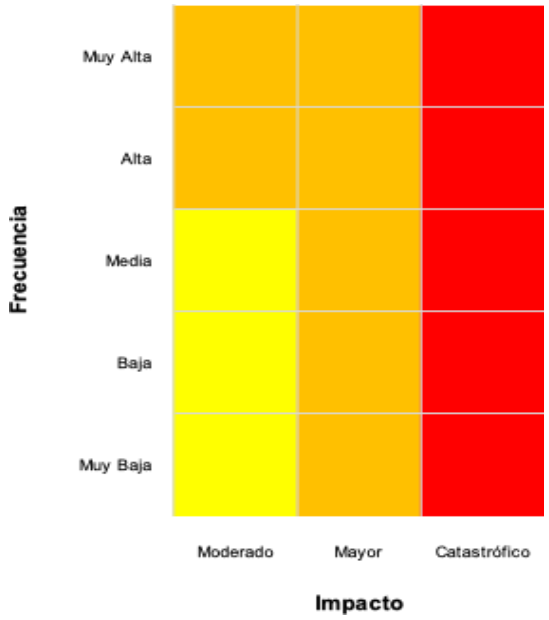


Figura 8: Matriz valoración del riesgo de corrupción

5.4.4 Definición de controles

Los controles se definen siguiendo los lineamientos para los riesgos operacionales. De la misma forma, su evaluación corresponde a la misma metodología descrita en el presente documento.

5.5. Lineamientos Para la Gestión de Riesgos de Seguridad de la Información

La política de seguridad y manejo de la información del IDEP se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI), alineado con el marco de referencia de arquitectura TI y la Política de Gobierno Digital.

Es necesario designar un responsable de la Seguridad de la Información quien definirá los lineamientos específicos correspondientes a la seguridad de la información, el cual debe pertenecer a una dependencia que haga parte de la Alta Gerencia o Línea estratégica de defensa. Los líderes de cada proceso y dependencia, previa identificación y valoración de sus activos de información, hacen parte del grupo responsable de Seguridad de la Información y por tanto deben seguir los lineamientos de gestión de riesgos de este documento.

De igual manera se requiere disponer de los recursos necesarios para el desarrollo de la gestión de riesgos de seguridad de la información con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad que serán formulados con base en la identificación de activos de la información.

5.5.1. Responsabilidad para la gestión de los activos de seguridad de la información

Proceso Gestión Tecnológica: responsable de apoyar metodológicamente a los procesos en el levantamiento del inventario de activos de información tecnológicos a su cargo, así como la identificación de los riesgos de seguridad de la información, sus controles y la forma de gestionarlos.

Proceso Gestión Documental: responsable de apoyar metodológicamente a los procesos en el levantamiento del inventario de activos de información documentales, así como de identificar en primera instancia, los riesgos de seguridad de la información, sus controles y la forma de gestionarlos.

Proceso Dirección y Planeación: es responsable de realizar acompañamiento metodológico en la identificación de los riesgos, así como realizar el monitoreo a la gestión de riesgos de seguridad de la información.

Dueños de los activos de información de cada proceso: son responsables del manejo de los activos de información y participan en el levantamiento del inventario de activos de información de su proceso, así como de la identificación de los riesgos de seguridad de la información.

5.5.2 Identificación de los activos de seguridad de la información

Para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

- **Activo de información (AI):** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma, que tenga valor para la organización y que por lo tanto deba proteger frente a los riesgos y amenazas para asegurar el correcto funcionamiento del negocio.

- **Importancia de identificar los activos:** determinar qué es lo más importante que la Entidad y sus procesos poseen y en este sentido saber qué es lo que debe proteger para garantizar su funcionamiento interno (Back Office) y de cara al ciudadano (Front Office).

La identificación y valoración de activos debe realizarse por parte de la primera línea de defensa en cada proceso donde aplique la gestión del riesgo de seguridad de la información, con la orientación del responsable de Seguridad de la Información de la entidad.

El siguiente esquema muestra los pasos para identificar los activos de información[1]:

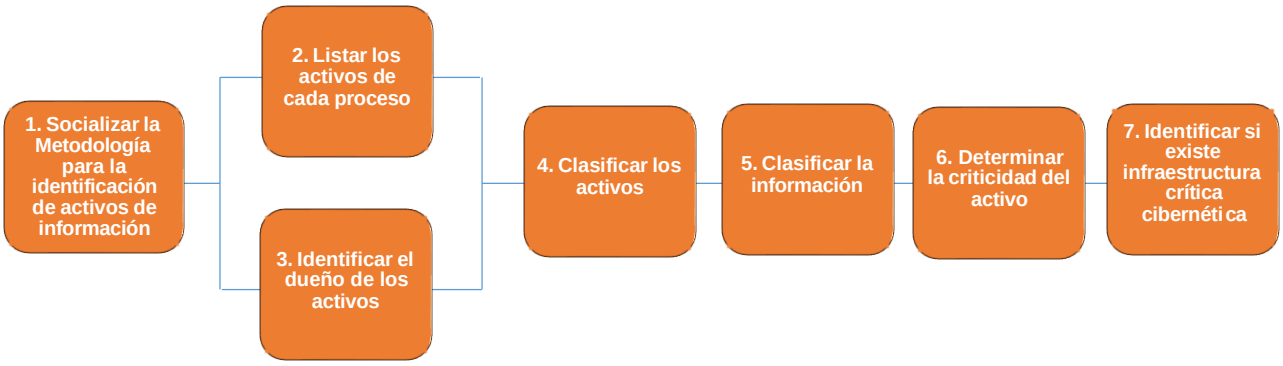


Figura 9. Esquema identificación de activos de información. Fuente: Elaboración propia

- **Paso 1 - Socializar la Metodología para la identificación de los activos de información:** de tal manera que los actores involucrados tengan claridad frente al despliegue de la metodología a seguir para realizar una adecuada identificación de los activos de información.

- **Paso 2 - Listar los activos de cada proceso:** se deben listar indicando un consecutivo, nombre y descripción breve de cada uno. Los activos de información deben de cumplir con los parámetros legales, normativos y de licenciamiento.

- **Paso 3 - Identificar el dueño de los activos:** se debe identificar al propietario de los activos. Generalmente es el Líder de Proceso o Jefe de área perteneciente al proceso.

- **Paso 4 - Clasificar los activos:** cada activo debe tener una clasificación[2] o pertenecer a un determinado grupo de activos según su naturaleza (información, software, hardware, servicios, intangibles, personas, instalaciones); la siguiente es una guía según su naturaleza[3].

Tipo de activo	Descripción
Información	Información almacenada 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

[1] Para la identificación de activos se puede tomar como referencia el Anexo "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas" del MINTIC.

[2] Clasificación de la información: se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada (Guía para la Gestión y Clasificación de Activos de Información- Mintic.

[3] Tomado del Anexo 4. Guía de Gestión de Riesgo de Seguridad Digital. 2018. Mintic

	información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	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). Incluyendo los servicios relacionados para la gestión del archivo de gestión y archivo central.
intangibles	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
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
Roles	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Tabla 16. Clasificación de activos. Fuente: Mintic

- **Paso 5 – Clasificar la información**: conforme a lo definido en las leyes 1712 de 2014 de transparencia y derecho al acceso a la información pública[4], 1581 de 2012 de Protección de datos personales[5] y el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos. Ejemplo:

Activo	Tipo de Activo	Ley 1712 de 2014	Ley 1581 de 2012
Factura de venta	Información	Información pública	Contiene datos personales
Software ERP	Software	Información pública clasificada	Contiene datos personales
Switch	Hardware	Información reservada	No contiene datos personales

Tabla 17. Elaboración propia

- **Paso 6 – Determinar la criticidad del activo:** se debe evaluar su criticidad para determinar el grado de importancia de cada uno. Esta criticidad se debe tener en cuenta en el análisis de riesgos para hacer una valoración adecuada.

[4] 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.
[5] Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

A continuación, se presentan los criterios de clasificación para determinar el nivel de los atributos de confidencialidad, integridad y disponibilidad de los activos de información[6]:

CONFIDENCIALIDAD	
Tipo de información	**Criterio**
Información Pública reservada Nivel: Alta (A)	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
Información Pública clasificada Nivel: Media (M)	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de ésta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
Información Pública Nivel: Baja (B)	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de Información pública reservada

Tabla 18. Clasificación de acuerdo con la Confidencialidad. Fuente: Mintic

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

Tabla 19. Clasificación de acuerdo con la Integridad. Fuente: Mintic

DISPONIBILIDAD	
Nivel	**Criterio**
Alta (A)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
Media (M)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
Baja (B)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad Alta.

Tabla 20. Clasificación de acuerdo con la Disponibilidad. Fuente: Mintic

[6] Tomado del Modelo de Seguridad y Privacidad de la Información MSPI (Clasificación de activos de información)

Una vez valorado el nivel de cada uno de los atributos de confidencialidad, integridad y disponibilidad, se determina su criticidad o importancia de acuerdo con las siguientes escalas:

NIVEL DE CRITICIDAD	
Nivel	**Criterio**
Alta	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
Media	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
Baja	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 21. Nivel de criticidad del activo de información. Fuentes: Mintic

- **Paso 7 – Identificar si existe infraestructura crítica cibernética (ICC):** Un activo es considerado crítico cuando su impacto o afectación supera alguno de los siguientes 3 criterios:

Tipo de impacto	Criterio
Impacto social	Afecta el 0,5% de la población nacional
Impacto económico	PIB de un Día o del 0,123% del PIB Anual
Impacto ambiental	3 años en recuperación

Tabla 22. Tipo de impacto en ICC. Fuente: Mintic

Inventario de activos de información: levantar e identificar el inventario de activos de información permite clasificar los activos a los cuales se les debe dar mayor protección. En términos generales los siguientes pasos se deben seguir para el levantamiento o actualización del inventario *(creación, modificación, eliminación de un activo)*: Definición, revisión, actualización, publicación. Siendo el producto final la Matriz de Inventario y clasificación de activos de información. De acuerdo con los pasos anteriores se presenta una guía de referencia para la elaboración del inventario de activo.

- **Definición:** consiste en determinar qué activos de información van a hacer parte del inventario. Para lo cual debe existir un equipo que realice la gestión de activos de información en la entidad y por medio del líder de cada proceso. Es recomendable que la definición se lleve a cabo **por lo menos una vez al año.**

#	Proceso	Activo	Descripción	Ubicación	Propiedad	Acceso	Gestión	Tipo de activo	Clasificación de información	Criticidad del activo
ID	Nombre del proceso al que pertenece el activo	Nombre del activo	Descripción clara del activo para facilitar su identificación	Descripción de la ubicación tanto física como electrónica del AI.	Dueño del AI: Propietario del AI. Custodio: parte designada de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario[7].	Son los usuarios que generan, obtienen, transforman, conservan, eliminan o utilizan la información, en medio físico, digital, a través de redes de datos o sistemas de información	Fecha de ingreso del AI al inventario Fecha de salida del AI del inventario	De acuerdo con su naturaleza: información, software, hardware, servicios, intangibles, componentes de red, personas, instalaciones.	La clasificación hace referencia a la protección de la información de acuerdo con: *Confidencialidad: [8] -Información pública reservada (Nivel Alto) -Información pública clasificada (Nivel Medio) -Información pública (Nivel Bajo) *Integridad (Nivel Alto, Medio, Bajo). *Disponibilidad (Nivel Alto, Medio, Bajo).	Es el cálculo automático que determina el valor general del activo según su Nivel de Clasificación (Alta, Media, Baja). Resulta de la calificación obtenida para confidencialidad, integridad y disponibilidad, conforme a los criterios para determinar la calificación final (Alta, Media, Baja).

Tabla 23. Ejemplo inventario de activos de información. Fuente: Elaboración propia basado en Guía 5 para la gestión y clasificación de activos de información

[7] Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

[8] De acuerdo con lo dispuesto en la Ley 1581 de 2012 de Protección de datos personales y la Ley 1712 de 2014 de Transparencia y del Derecho de Acceso a la Información Pública

- **Revisión:** se refiere a la verificación para determinar si un activo de información continúa haciendo parte o no del inventario o si se requiere actualizar los valores de evaluación y clasificación de activos. En general puede ser revisado o validado en cualquier momento que el Líder de proceso, el Proceso de Gestión Tecnológica, Proceso de Gestión Documental o el Oficial de Seguridad de la Información lo consideren pertinente.

- **Actualización:** una vez identificados los cambios a realizar en el inventario se procede a actualizar el inventario de activos de información del respectivo proceso.

- **Publicación:** el inventario de activos de información se clasifica como **"confidencial**" y sólo estará disponible a los servidores de la EMB en la herramienta definida en el Sistema Integrado de Gestión.

5.5.3 Identificación del Riesgo

Para la identificación de los riesgos de Seguridad de la Información se aplican las fases definidas para los riesgos operacionales mencionadas previamente en este documento.

5.5.3.1 Análisis de Objetivos Estratégicos y de los Procesos

El análisis de objetivos estratégicos y de los procesos de los riesgos de seguridad de la información toma en cuenta los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

5.5.3.2 Identificación de los Puntos de Riesgo

La identificación de los puntos de riesgo de los riesgos de seguridad de la información toma en cuenta los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

5.5.3.3 Identificación de áreas de impacto

La identificación de áreas de impacto de los riesgos de seguridad de la información toma en cuenta los mismos criterios utilizados para los riesgos de gestión y mencionados de manera previa en este documento.

5.5.3.4 Identificación de áreas de factores de riesgo

La identificación de áreas de factores de riesgo de los riesgos de seguridad de la información toma en cuenta los mismos criterios utilizados para los riesgos operacionales mencionadas previamente en este documento.

5.5.3.5 Descripción del riesgo

Independiente de la tipología la descripción del riesgo debe ser lo suficientemente clara sin dar lugar a ambigüedades tanto para el líder del proceso como para personas ajenas al proceso. Para una adecuada redacción del riesgo se siguen las mismas premisas establecidas en este documento.
Se podrán identificar los siguientes tres riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad,

- Pérdida de la integridad,
- Pérdida de la disponibilidad[9].

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y de manera conjunta analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Es decir que se deben agrupar activos del mismo tipo, ejemplo: analizar conjuntamente activos de software para determinar amenazas y vulnerabilidades comunes que pueden afectar a dicho grupo.

Una amenaza es un evento o acción que puede producir un daño material o inmaterial sobre los elementos de un sistema (activos de información).

Una vulnerabilidad es una falla o debilidad que pone en riesgo la seguridad de la información. **La presencia de una vulnerabilidad en si no genera ningún daño,** es necesario que una amenaza pueda explotar la debilidad.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Asignación errada de los derechos de acceso	Abuso de los derechos
Información	Falta de controles de acceso físico	Hurto de información
Personas	Falta de capacitación en las herramientas	Error en el uso

Tabla 24. Amenazas y vulnerabilidades por activo de información

Por ende, el riesgo de seguridad de la información (RI) se asocia al potencial que tiene una amenaza para explotar una vulnerabilidad para generar una pérdida o daño en un activo de información o grupo de activos de información.

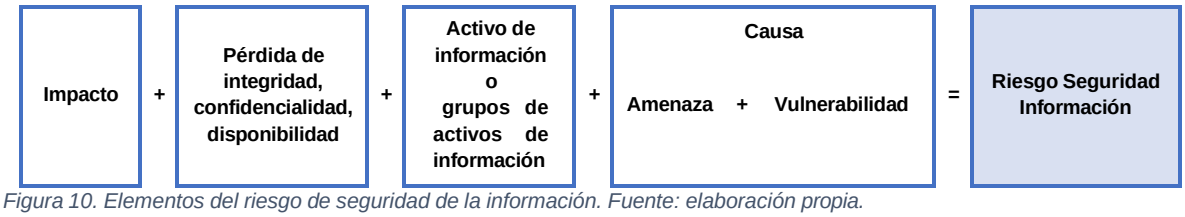


Figura 10. Elementos del riesgo de seguridad de la información. Fuente: elaboración propia.

Se propone una estructura que facilita su redacción y claridad que inicia con la frase "Posibilidad de" y se analizan los siguientes aspectos:

[9] Se puede tomar como guía el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas - Mintic.

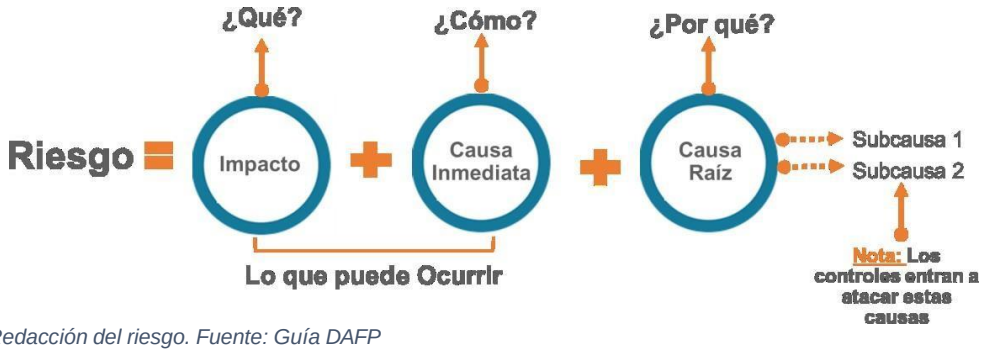


Figura 11. Redacción del riesgo. Fuente: Guía DAFP

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

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, lasmismas 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 teneren cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Ejemplo de Redacción del Riesgo:

Riesgo	Activo	Descripción del Riesgo	Amenaza	Causa /Vulnerabilidades	Consecuencias
Pérdida de integridad	Base de Datos de nómina	Posibilidad de impacto reputacional y/o económico por la pérdida de integridad de la base de datos de nómina debido a la modificación no autorizada por la falta de Políticas de seguridad y de control de acceso y autenticación débil.	Modificación no autorizada	Falta de Políticas de seguridad y de control de acceso Autenticación débil	Impacto reputacional o económico
Pérdida de Integridad	Expediente de predios	Posibilidad de impacto reputacional y/o económico por la pérdida de integridad de los expedientes de los predios debido al hurto de información por la ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad.	Hurto de información	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Impacto reputacional o económico

Tabla 25. Ejemplo riesgo de seguridad de la información. Fuente: elaboración propia

5.5.3.6 Clasificación del riesgo

La clasificación de los riesgos de seguridad de la información toma en cuenta los mismos criterios utilizados para los riesgos operacionales mencionados previamente.

5.5.4 Valoración del riesgo

La valoración de los riesgos de seguridad de la información toma en cuenta los mismos criterios para calificar la probabilidad y el impacto, utilizados para la valoración de los riesgos operacionales mencionados previamente en este documento.

5.5.4.1 Análisis de riesgos

Para determinar la probabilidad y el impacto en el análisis de los riesgos de seguridad de la información, se consideran los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

Nota: Para los riesgos de seguridad de la información se debe tener en cuenta que la probabilidad y el impacto se determinan con base en la amenaza **no** en las vulnerabilidades.

5.5.4.2 Evaluación del riesgo

La evaluación de los riesgos de seguridad de la información considera los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

Nota: Para la identificación de los controles asociados a los riesgos de seguridad de la información, se puede tomar como una guía de referencia el Anexo A de la norma NTC: ISO/IEC 27001[10], sin embargo, se aclara que se puede implementar también otros controles que no estén dentro del anexo, así como lo controles definidos en los procedimientos internos del IDEP relacionados con la gestión documental. Se tendrán en cuenta las características de diseño y valoración de los controles de los riesgos de gestión y mencionados de manera previa en este documento.

5.5.4.3 Tratamiento del riesgo

Las opciones de tratamiento y formulación de planes de acción para los riesgos de seguridad de la información consideran los mismos criterios utilizados para los riesgos de gestión y mencionados de manera previa en este documento.

5.5.4.4 Herramientas para la Gestión

Como herramientas de gestión para el autocontrol y monitoreo de los riesgos de seguridad de la información, se aplican los mismos criterios utilizados en los riesgos de gestión y mencionados de manera previa en este documento.

5.5.4.5 Monitoreo y Revisión

Las actividades de monitoreo y revisión son transversales en todas las etapas de la gestión de riesgos de seguridad de la información, y se aplican los mismos criterios utilizados en los riesgos de gestión y mencionados de manera previa en este documento.

[10] Anexo A de la norma NTC: ISO/IEC 27001 se menciona dentro Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.

5.6. Lineamientos para la Gestión de Riesgo Fiscal

5.6.1 Identificación del Riesgo

El riesgo fiscal es el efecto dañoso sobre los recursos públicos o los bienes o intereses patrimoniales de naturaleza pública, a causa de un ***evento potencial***.

Los elementos que componen la definición son los siguientes:

- **Efecto:** Es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

- **Evento Potencial:** se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. El evento potencial es equivalente a la causa raíz.

En ese orden de ideas el riesgo fiscal se puede resumir así:

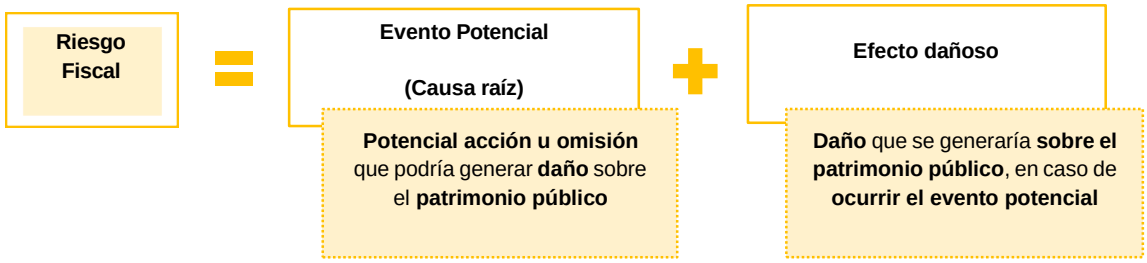


Figura 12. Estructura del riesgo fiscal. Fuente: Elaboración propia (basado DAFP)

Para la identificación de los riesgos fiscales se aplican las mismas fases utilizadas para los riesgos operacionales mencionados previamente en este documento.

5.6.1.1 Análisis de objetivos estratégicos y de los procesos

El análisis de objetivos estratégicos y de los procesos de los riesgos fiscales toma en cuenta los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

5.6.1.2 Identificación de los puntos de riesgo fiscal y las circunstancias Inmediatas

Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Las circunstancias inmediatas, son aquellas situaciones o actividades bajo la cual se

presenta el riesgo, pero no constituyen la causa principal o básica “causa raíz” para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Para identificar los puntos de riesgo y las circunstancias inmediatas, se puede realizar un taller entre el nivel directivo, asesores y aquellos servidores y contratistas que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal *(actividades de gestión fiscal*[11] *en las que potencialmente se genera riesgo fiscal)* y circunstancias Inmediatas *(situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal).*

La Guía de Riesgos del DAFP propone las siguientes preguntas orientadoras:

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal?
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.

[11] **Actividades de gestión fiscal:** actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

Sirve para identificar	Preguntas y respuestas para la identificación
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del *"¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" del Anexo 1 de la Guía DAFP, son aplicables a la entidad?*

Tabla 26. Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas. Fuente: Guía DAFP

5.6.1.3 Identificación de áreas de impacto

Para el riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que **no son riesgos fiscales**, los siguientes:

a. Los riesgos de daño antijurídico, riesgo de pago de condenas y conciliaciones.
b. Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales es tener claro el concepto de patrimonio público y de las expresiones que hacen parte de dicha definición: bienes públicos, recursos públicos, intereses patrimoniales de naturaleza pública.

5.6.1.4 Identificación de áreas de factores de riesgo

La identificación de áreas de factores de riesgo de los riesgos fiscales toma en cuenta los mismos criterios utilizados para los riesgos de gestión y mencionados de manera previa en este documento.

5.6.1.5 Descripción del riesgo

Independiente de la tipología la descripción del riesgo debe ser lo suficientemente clara sin dar lugar a ambigüedades tanto para el líder del proceso como para personas ajenas al proceso. Para una adecuada redacción del riesgo se siguen las premisas establecidas en este documento.

La **causa raíz** corresponde a cualquier evento potencial **(acción u omisión)** que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro.

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

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador (causa), y otro es el daño (efecto).

Para redactar un riesgo fiscal se debe tener en cuenta:

- **Iniciar con la oración**: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
- **Impacto (Qué):** Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- **Circunstancia inmediata (Cómo):** Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
- **Causa Raíz (Por qué):** es el evento potencial (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada.

Por lo anterior la estructura para la redacción del riesgo fiscal sería la siguiente:

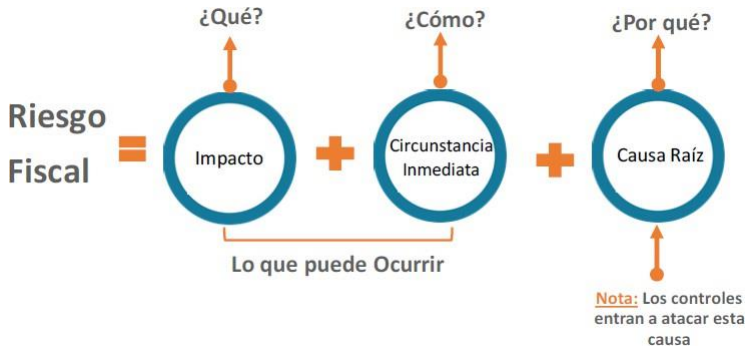


Figura 15. Redacción del riesgo. Fuente: Guía DAFP

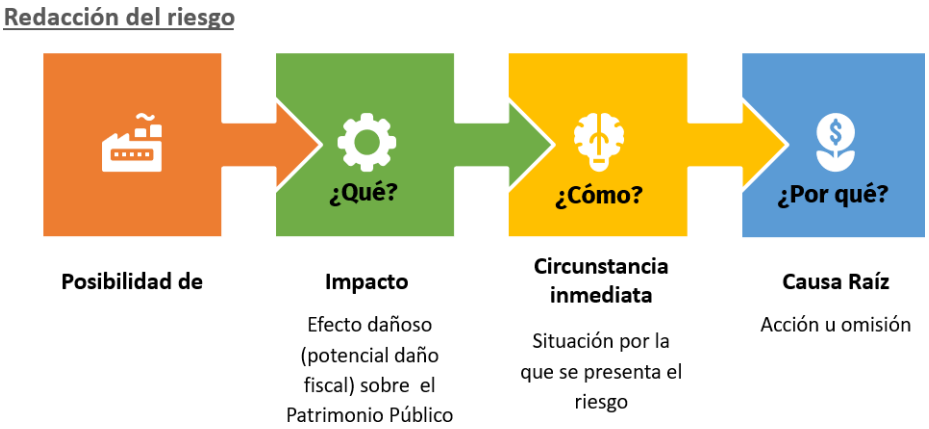


Figura 16. Redacción del riesgo. Fuente: Elaboración propia (basado DAFP)

Ejemplos:

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

Tabla 27. Ejemplos de riesgos Fiscales.

5.6.1.6 Clasificación del riesgo

La clasificación del riesgo fiscal toma en cuenta los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

5.6.2 Valoración del riesgo

La valoración del riesgo fiscal toma en cuenta los mismos criterios para calificar tanto probabilidad como el impacto, utilizados para la valoración de los riesgos operacionales mencionados previamente en este documento.

5.6.2.1 Análisis de riesgos

Para determinar la probabilidad y el impacto en el análisis de los riesgos fiscales, se consideran los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

Nota: Considerando la naturaleza y alcance del riesgo fiscal, éste **siempre tendrá un impacto económico**, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal.

5.6.2.2 Evaluación del riesgo

La evaluación del riesgo fiscal considera los mismos criterios utilizados para los riesgos operacionales mencionados previamente en este documento.

5.6.2.3 Tratamiento del riesgo

Las opciones de tratamiento del riesgo fiscal y formulación de planes de tratamiento, toma en cuenta los mismos criterios utilizados para la valoración de los riesgos operacionales mencionados previamente en este documento.

5.6.2.4 Herramientas para la Gestión

Como herramientas de gestión para el autocontrol y monitoreo de los riesgos fiscales, se aplican los mismos criterios utilizados en los riesgos operacionales mencionados previamente en este documento.

5.6.2.5 Monitoreo y Revisión

Las actividades de monitoreo y revisión son transversales en todas las etapas de la gestión de los riesgos fiscales y se aplican los mismos criterios utilizados en los riesgos de gestión y mencionados de manera previa en este documento.

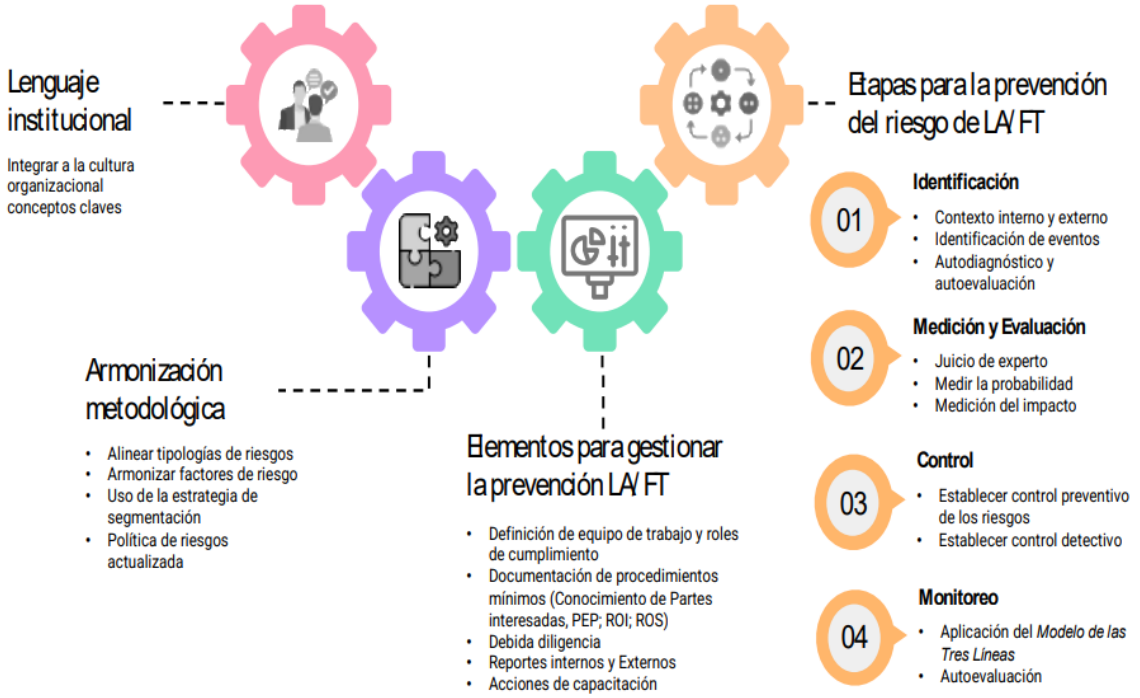
5.7 Lineamientos para la Gestión de Lavado de Activos y Financiación del Terrorismo LA/FT

En el sector público distrital se entiende por riesgo de LA/FT/FPADM la posibilidad de pérdida o daño que puede sufrir una entidad por su propensión a ser utilizada directa o indirectamente a través de sus operaciones como instrumento para el lavado de activos, canalización de recursos hacia la realización de actividades terroristas y/o financiación de armas de destrucción masiva, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

5.7.1 Sistemas de administración de riesgos LA/FT/FPADM

La adaptación e implementación de los siguientes aspectos promoverá la prevención, detección y el reporte de las operaciones sospechosas vinculadas al LA/FT y promoverá el control de operaciones ilícitas como soborno, cohecho, nepotismo u otros comportamientos inapropiados que puedan cometer abusivamente algunos servidores o colaboradores públicos, así la entidad cuente con controles, es decir, bajo su propia responsabilidad individual. A continuación, se ilustra los principales aspectos de adopción e implementación sugeridos en el presente documento, y que facilitaran a las entidades del distrito capital alinearse a este deber institucional:

Figura 16. Adaptación del modelo SAELAFT



Fuente: Secretaría General (Dirección Distrital de Desarrollo Institucional)

5.7.2 Conceptos claves para la adaptación del sistema de administración de riesgo LA/FT

El lavado de activos, y la financiación del terrorismo y la proliferación de armas de destrucción masiva, se presentan actualmente como problemas complejos y difícilmente abordables, que no tienen soluciones inmediatas y que se constituyen en flagelos que afectan directamente las estructuras económicas de las naciones, lo cual tiene un impacto territorial, nacional y mundial.

Es importante reconocer que tanto el lavado de activos como la financiación del terrorismo son delitos tipificados en el Código Penal colombiano, por lo que a continuación se presenta su definición para una mayor claridad y comprensión de las entidades para la identificación de riesgos asociados a delitos.

5.7.2.1 Lavado de activos (LA)

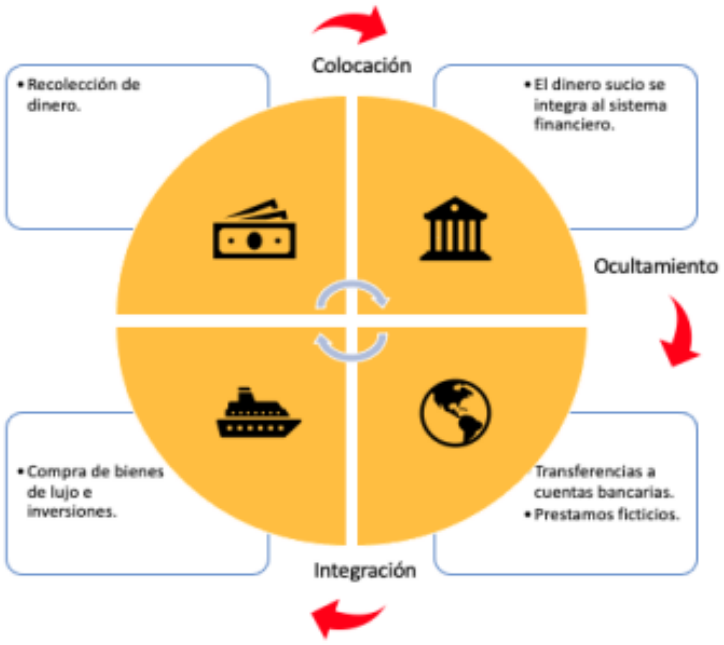
De conformidad con lo estipulado en el artículo 323 de la Ley 599 de 2000, modificado por el artículo 11 de la Ley 1762 del 10 de julio de 2015, el lavado de activos se refiere a quien "adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, contrabando, contrabando de hidrocarburos o sus derivados, fraude aduanero o favorecimiento y facilitación del contrabando, favorecimiento de contrabando de hidrocarburos o sus derivados, en cualquiera de sus formas, o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito (…)".

5.7.2.1.1 Etapas del lavado de activos

- Colocación: es la disposición física del dinero en efectivo proveniente de actividades delictivas. Durante esta fase inicial, el lavador de dinero introduce sus fondos ilegales en actividades legales o aparentemente legales, bien a través del sistema financiero o de otros tipos de negocios o contratos, tanto nacionales como internacionales.
- Estratificación / Ocultamiento: es la separación de fondos ilícitos de su fuente mediante una serie de transacciones, cuyo fin es desdibujar la transacción ilícita original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras6 para disimular el rastro documentado, la fuente y la propiedad de los fondos.

- Integración: es dar apariencia legítima a riqueza ilícita mediante el reingreso en la economía con transacciones comerciales o personales que aparentan ser normales. Esta fase conlleva la colocación de los fondos lavados de vuelta en la economía para crear una percepción de legitimidad. El lavador podría optar por invertir los fondos en bienes raíces, artículos de lujo o proyectos comerciales, entre otros.

Figura 17. Esquema de Lavado de Activos. Fuente: Secretaría General, Subsecretaría Distrital de Fortalecimiento Institucional con base en esquema de Oficina de las Naciones Unidas contra las Drogas y el Delito.



5.7.2.2 Financiación del terrorismo (FT)

De conformidad con lo estipulado en el artículo 345 de la Ley 599 de 2000, modificado por el artículo 16 de la Ley 1453 de 2011, la financiación del terrorismo se refiere a quien “directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas”.

5.7.2.2.2 Etapas de la Financiación del Terrorismo

- Recaudación / Recolección: consiste en la búsqueda de fuentes de financiación por las organizaciones terroristas, bien sean de origen legal, como los aportes de los Estados, individuos, entidades, organizaciones y donantes en general que apoyan su causa o son engañados, así como recursos provenientes de cualquier actividad delictiva, fondos que generalmente circulan en efectivo.

- Disposición / Transmisión: es la fase intermedia que busca poner el dinero recaudado a disposición de la organización terrorista, quedando simplemente la espera de su utilización final; corresponde al movimiento de los fondos a través de distintas técnicas, se trata de ocultar sus movimientos y destino final.
- Utilización / Uso: fase donde los fondos se utilizan básicamente para la financiación de la logística estructural de la organización o la logística operativa en materia de planeación y ejecución de actos terroristas.

Figura 18. Esquema de Financiación del Terrorismo. Fuente: Secretaría General, Subsecretaría Distrital de Fortalecimiento Institucional con base en esquema de Oficina de las Naciones Unidas contra las Drogas y el Delito.

5.7.3 Sistemas de administración de riesgos LA/FT

Un Sistema de Administración de Riesgos en Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva está compuesto por varios componentes que contribuyen a promover la cultura de gestión del riesgo en las entidades, con el fin de prevenir que las mismas puedan ser utilizadas por terceros para dar apariencia de legalidad a recursos ilícitos originados de actividades delictivas y/o para canalizar recursos hacia la realización de actividades terroristas.

Dependiendo de la naturaleza de cada entidad y de la superintendencia u órgano que las vigila, supervisa y controla (para el caso de las obligadas), se cuenta con tres (3) tipos de sistemas de administración de riesgos, los cuales tienen diferentes niveles de exigencia en la aplicación de requisitos. A continuación, se describen de manera general los tres (3) sistemas vigentes:

a. SARLAFT EL Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo, es un sistema pensado en consonancia con los estándares internacionales proferidos por el Grupo de Acción Financiera Internacional (GAFI), y fue expedido en el 2008 por la Superintendencia Financiera de Colombia (SFC), como base para que otras entidades de supervisión y reguladores emitieran normas referentes a esta materia. Los requisitos establecidos para el SARLAFT se rigen por la circular 027 de 2020 expedida por la Superintendencia Financiera de Colombia, que otorgó el nombre al sistema de SARLAFT 4.0, el cual cuenta con unas actualizaciones normativas en cuanto a aspectos tales como: gestión de nuevos factores de riesgo, validación de nuevas listas vinculantes y mayor precisión en cuando al conocimiento del beneficiario final, entre otros.

b. SAGRILAFT El Sistema de Autocontrol y Gestión del Riesgo Integral de LA/FT/FPADM, es el sistema establecido por la Superintendencia de Sociedades y que proporciona estándares para que sus entidades supervisadas adopten medidas que les permitan "la identificación, segmentación, calificación, individualización, control y actualización de los factores de riesgos y los riesgos asociados a la probabilidad de que éstas puedan ser usadas o puedan prestarse como medio en actividades relacionadas con el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas destrucción masiva".

Actualmente los requisitos establecidos para el SAGRILAFT se encuentran recogidos en el Capítulo X de la Circular Básica Jurídica de la Superintendencia de Sociedades.

c. SIPLAFT El Sistema Integral para la Prevención y Control del Lavado de Activos y la Financiación del Terrorismo, es el sistema establecido por el Consejo Nacional de Juegos y Azar (CNJSA) que proporciona estándares para sus entidades vigiladas establezcan actividades de prevención y control para el lavado de activos y la financiación del terrorismo. Actualmente, los requisitos establecidos para el SIPLAFT se encuentran vigentes mediante el Acuerdo 574 de 2021 expedida por el CNJSA.

5.7.3.1 Delitos fuente

Para la realización de las actividades tendientes a ocultar dinero de origen ilegal y darle posterior apariencia de legalidad a través de su vinculación al sistema económico, existen actividades delictivas a partir de las cuales se obtienen aquellos recursos ilícitos que se pretenden lavar. Dichas actividades son denominadas delitos fuente o delitos subyacentes y se encuentran determinadas en el art. 323 de la Ley 599 de 2000, modificada por el artículo 11 de la Ley 1762 de 2015, que tipifica el delito de lavado de activos en Colombia.

Cuando se habla de actividades ilegales generalmente se señala el narcotráfico como principal delito del LA/FT. Sin embargo, la Ley 599 de 2000 (Código Penal colombiano) contempla otras actuaciones prohibidas generadoras de recursos ilícitos, entre las que se encuentran:

▪ 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 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).

Respecto al tema, el plan de acción del CONPES 01 de 2019 "Política Pública Distrital de Transparencia, Integridad y no Tolerancia con la Corrupción", contempla el LA/FT en relación con los actos conexos a corrupción, que pueden ser aquellos delitos contra la administración pública. Por ello es necesario tener un panorama general de las actuaciones ilegales, que permitan enlazar los agentes generadores de riesgo, la identificación de señales de alerta y los delitos generadores de recursos ilícitos. Ello puede lograrse, en principio, adelantando una validación general del contexto normativo vigente, respecto de los delitos contra la administración pública y aquellos vinculados al lavado de activos y la financiación del terrorismo.

5.7.4 Factores críticos en la prevención de LA/FT

Son aquellas situaciones, que, al ser analizadas, se salen de los comportamientos particulares de las contrapartes, considerándose atípicas y que, por tanto, requieren mayor análisis para determinar si existe una posible operación de lavado de activos o financiación del terrorismo (UIAF, 2021). Cada factor de riesgo debe tener sus respectivas señales de alerta para facilitar su comprensión. El agente generador de riesgo (lavador 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. Las organizaciones ilegales que se dedican al lavado de activos pueden utilizar a personas de escasos recursos, así como a personas de altos ingresos, pues su finalidad es utilizarlas para dar apariencia de legalidad a los recursos de origen ilícito.

5.7.5 Adaptación en la gestión de riesgos LA/FT

Los riesgos están referidos al flujo de LA/FT, en el que el lavador puede acudir a la entidad para transformar el dinero producto de cometer actividades ilícitas utilizando los canales o medios que ofrecen las instituciones y disfrutar de las ganancias ilícitas, como se muestra en la ilustración. Buscamos que las matrices de riesgos identifiquen el riesgo de LA/FT/FPADM que se pueden llegar a materializar a través de riesgos asociados.

Figura 19. Flujo de LA/FT. Fuente: Secretaría General- Dirección Distrital de Desarrollo Institucional

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas internas de gestión bajo el Modelo Integrado de Planeación y Gestión (MIGP), procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. La gestión de los riesgos del LA/FT/FPADM no requiere la utilización de metodologías particulares. Quienes diseñan y modelan las matrices de riesgos institucionales pueden gestionar los riesgos de operaciones indebidas; es decir, no hay metodologías especiales para identificar riesgos, por el contrario, se deben utilizar técnicas normalmente aceptadas y conocidas por las entidades, las cuales generalmente tienen su principal referente en la Guía de Administración de Riesgos de Función Pública (DAFP).