Igualdad

POLITICA DE ADMINISTRACIÓN DE RIESGOS 03/12/2024

RESUMEN:

La política de Administración de Riesgos del Ministerio de Igualdad y Equidad de Colombia se ha elaborado con el objetivo de proporcionar un marco integral y sistemático para la gestión de riesgos dentro del Ministerio, así como asegurar que todas las actividades y procesos se desarrollen con una clara comprensión de los posibles riesgos, implementando estrategias efectivas para identificarlos, evaluarlos, mitigarlos y monitorearlos.

La política de Administración de Riesgo establece las directrices vinculantes para todas las dependencias del Ministerio, las direcciones regionales y las áreas que ejecutan procesos tercerizados, en concordancia con la estructura ministerial definida en el Decreto 1075 de 2024. Estas políticas son de obligatorio cumplimiento y su implementación debe ser supervisada y documentada por todos los servidores públicos, contratistas y terceros que participen en los procesos institucionales, garantizando así una gestión integral y estandarizada de los riesgos en todos los niveles de la organización.

Palabras clave: Politicas-Riesgo- Controles-Impacto-Guías-Corrupción-

Contenido

INDICE DE TABLA

INDICE DE ESQUEMAS

1. INTRODUCCIÓN

La presente política tiene como finalidad establecer la política y las directrices para la adecuada administración de riesgos y define la metodología para la identificación, análisis, valoración, establecimiento de controles, tratamiento y seguimiento de los riesgos inherentes a los procesos, relacionados con los riesgos de gestión, de corrupción y de seguridad digital, con el propósito de evitar que interfieran en el cumplimiento de los objetivos y misión institucional.

El Comité Institucional de Coordinación de Control Interno , en sesión del día 03 de diciembre del 2024, aprobó y adoptó la Política de Administración de Riesgos para el Ministerio de Igualdad y Equidad en donde se incluye la Política y metodología para los riesgos de Seguridad Digital, como parte integral de la gestión de riesgos, los cuales hacen parte de la estrategia de gobierno digital para la implementación de un modelo de seguridad y privacidad de la información – MPSI en las entidades públicas, permitiendo al Ministerio de Igualdad y Equidad su correcto desempeño dentro de la política pública y resguardando su información de cualquier tipo de alteración, mal uso o perdida, así como permitir la toma de decisiones.

El Comité Institucional de Coordinación de Control Interno, adopta la metodología de Gestión de Riesgos para las entidades públicas establecida por el Departamento Administrativo de la Función Pública-DAFP, conforme a los nuevos lineamientos dados a través de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas.

La administración de riesgos de Ministerio de Igualdad y Equidad, se enmarca en lo dispuesto en el artículo 2.2.23.2 del Decreto 1499 de 2017, el cual actualiza del Modelo Estándar de Control Interno, a través del Manual Operativo del Modelo Integrado de Planeación y Gestión- MIPG, el artículo 4º del Decreto 1537 de 2001 el cual determina que la administración del riesgo, es parte integral del fortalecimiento del Sistema de Control Interno en las entidades públicas y define que las autoridades correspondientes, deberán establecer y aplicar políticas para su gestión; y el CONPES 3854 del 11 de abril de 2016, el cual establece la Política Nacional de Seguridad Digital que permite fortalecer las capacidades de la

entidades públicas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

La Entidad, contempla la Gestión del Riesgo como parte de la implementación del Modelo Integrado de Planeación y Gestión(MIPG), el cual establece la gestión del riesgo en las Políticas de: Planeación Institucional, la cual hace énfasis en la formulación de la Política de Administración de Riesgos; Política de Seguridad Digital, que define los aspectos a tener en cuenta para asegurar los activos de información de las entidades públicas y la Política de Control Interno, la cual establece en el Modelo Estándar de Control Interno-MECI, las responsabilidades de las diferentes instancias de las Entidades, conforme a las tres líneas de defensa.

El Ministerio de Igualdad y Equidad, adopta la metodología para la Administración de Riesgos, de acuerdo con los estándares establecidos por el Departamento Administrativo de la Función Pública (DAFP) en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. V4." V.6-2022 y sus anexos.

La Política de Administración de Riesgos establece las directrices vinculantes para todas las dependencias del Ministerio, las direcciones regionales y las áreas que ejecutan procesos tercerizados, en concordancia con la estructura ministerial definida en el Decreto 1075 de 2024. Estas políticas son de obligatorio cumplimiento y su implementación debe ser supervisada y documentada por todos los servidores públicos, contratistas y terceros que participen en los procesos institucionales, garantizando así una gestión integral y estandarizada de los riesgos en todos los niveles de la organización.

2. OBJETIVO GENERAL

Establecer los lineamientos para la administración de los riesgos de gestión, corrupción y seguridad digital asociados a la gestión institucional.

2.1 Objetivos Específico

- Comunicar a todos los niveles de la Unidad los lineamientos para la administración del riesgo, para promover su aplicación.

- Fomentar la cultura de la prevención del riesgo en todos los niveles de la Institución.
- Asignar responsabilidades frente a la administración del riesgo.

3. ALCANCE

El ámbito de aplicación de esta política abarca todas las dependencias, procesos y actividades del Ministerio de Igualdad y Equidad de Colombia. La política es aplicable a todos los niveles jerárquicos y funcionales del mismo. Este documento guía la gestión de riesgos en todas las áreas operativas, desde la planificación y ejecución de programas hasta la administración y cumplimiento normativo.

4. DEFINICIONES Y SIGLAS

Las definiciones y términos que se presentan a continuación han sido tomadas de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública (DAFP) versión 6 y del Anexo 4. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

Activo de información: 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.

Actividad de control: Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

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

Análisis de Riesgo: Determinar el impacto y la probabilidad del riesgo, dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

Apetito al 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.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales.

Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques.

Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

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.

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

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

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

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.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Fraude: Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Gestión del riesgo: Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

ICC: Es la denominación de lo que el CCOCI ha definido como Infraestructuras Críticas Cibernéticas en el ámbito colombiano.

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo.

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

Integridad: Propiedad de la información de ser exacta y completa.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas, entre otras.

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.

Líder o responsable del proceso: Persona con la responsabilidad y autoridad para gestionar un riesgo.

Mapa de Riesgos: Documento con la información resultante de la gestión del riesgo.

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.

Plan de contingencia: Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.

Plan de manejo del riesgo: Plan de acción propuesto por el grupo de trabajo interno, cuya evaluación de beneficio costo resulta positiva y es aprobado por la Alta Dirección.

Política de Administración de Riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

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

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Recurso Público: entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de

entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

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

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por eficiencias, 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 poder desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Fraude: Efecto que se causa sobre los objetivos de las entidades debido a una acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de Seguridad Digital: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo Fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

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.

Tolerancia al riesgo (niveles de aceptación): Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes, que específicamente para el riesgo de corrupción la tolerancia es ***inaceptable.***

Valorar el riesgo: Permite establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial. (Riesgo Inherente).

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. MARCO NORMATIVO

La gestión de riesgos en el sector público en Colombia se enmarca dentro de un conjunto de legislaciones y normativas que regulan y guían las prácticas de gestión de riesgos. A continuación, se detallan las principales normativas aplicables:

Artículo 2º, literal a, de la 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.

Ley 1474 de 2011. Estatuto Anticorrupción.

Ley 1712 de 2014. Ley de transparencia y acceso a la información pública.

Decreto 1081 de 2015. Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.

Decreto 1083 de 2015, artículo 2.2.21.5.4 Administración de riesgos**.**

Decreto 1499 de 2017. Actualiza el Modelo Estándar de Control Interno (MECI).

Guía para la administración del riesgo y el diseño de controles en entidades públicas. V.6. noviembre de 2022. Departamento Administrativo de la Función Pública (DAFP).

Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas- Anexo 4- DAFP. Agosto 2019

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

Guía No.7 Seguridad y Privacidad Información-MINTIC-2016.

Protocolo Identificación Riesgos corrupción Tramites- Anexo 3-DAFP diciembre 2018.

NTC-ISO 31000-2018. Gestión del Riesgo, principios y directrices.

CONPES 3854 Política Nacional de Seguridad Digital 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. Esta ley resalta la importancia de la gestión de riesgos como parte integral del control interno.

6. POLÍTICA PARA LA ADMINISTRACIÓN DE RIESGOS

6.1 Política general

El Ministerio de la Igualdad y Equidad está comprometido con llevar a cabo una gestión integral de riesgos que facilite el cumplimiento de la misión, los objetivos estratégicos, objetivos de los procesos y la satisfacción de los grupos de interés, llevando a cabo la identificación de riesgos de gestión por proceso, los riesgos de corrupción y los riesgos de seguridad digital, su análisis, valoración y formulación de los planes de tratamiento de riesgos o acciones para prevenir su ocurrencia o mitigar el impacto. Las políticas de manejo de riesgo aplican a todos los procesos de la entidad y establecen las opciones para el tratamiento de los riesgos. Los riesgos de corrupción son inaceptables y en consecuencia no se pueden asumir. El tratamiento general para los riesgos corresponde a la implementación de acciones que conlleven a reducir, evitar, compartir, aceptar o transferir y serán individuales para cada uno de los riesgos identificados. Las acciones o controles se formularán considerando su viabilidad técnica, económica y legal.

6.2 Políticas específicas

6.2.1 Política gobierno de riesgos

a) El Equipo Directivo asume el compromiso de establecer una adecuada estructura organizacional en la Unidad que soporte el sistema de gestión integral de riesgos y validar los avances en el aseguramiento y nivel de madurez del mismo.

b) El Equipo Directivo define el nivel de apetito al riesgo como "Bajo" y de cero tolerancias a los riesgos de corrupción, lineamiento con el cual se regirán todos los procesos, los cuales deberán garantizar un adecuado tratamiento de los riesgos residuales que se encuentren en niveles no admisibles.

c) El Equipo Directivo establece que todos los funcionarios de Ministerio de la Igualdad y Equidad hacen parte esencial en la gestión de los riesgos corporativos y que la responsabilidad puntual por la administración, tratamiento, indicadores y materializaciones de riesgos recae sobre los dueños de proceso, en línea con el Equipo de Gestión de Riesgos.

d) La gestión de riesgos está asegurada por tres líneas de defensa avaladas por la Dirección General están conformadas así:

- Primera Línea de Defensa: directores de las áreas, Coordinadores, líderes y ejecutores del proceso que ejercen autocontrol.

- Segunda Línea de Defensa: La Oficina Asesora de Planeación en coordinación con las personas que ejercen la dirección de la dependencia, en especial aquellas que son líderes de política o líderes de los subsistemas SIG-MIPG

- Tercera Línea de Defensa: Oficina de Control Interno

6.2.2 Política cultura de riesgos

Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno dispone de los recursos necesarios para el impulso, fortalecimiento y mantenimiento de la cultura de gestión de riesgos al interior de todos los procesos del Ministerio, dando los lineamientos para establecer las herramientas que deben ser implementadas para la identificación,

análisis, evaluación, tratamiento, monitoreo y comunicación de los diferentes tipos de riesgos a los que está expuesta.

El Equipo de Gestión de Riesgos impulsa la gestión unificada de los diferentes tipos de riesgos a nivel de todo el Ministerio y promueve las directrices, herramientas y metodologías para la articulación de los diferentes elementos de administración de riesgos en la cultura corporativa propendiendo por el aseguramiento y control de los procesos.

6.2.3 Política de cumplimiento de normatividad interna y externa relacionadas con la administración de riesgos

El Comité Institucional de Gestión y Desempeño, Comité Institucional de Control Interno establecen las políticas, normas, lineamientos y directrices para la Institucional adecuada administración de los riesgos, para el aseguramiento de los procesos y la consecución de los objetivos estratégicos y de procesos tomando como referencia los diferentes marcos y estándares normativos que enmarcan a los sistemas de administración de riesgos entre estos: Estatuto anticorrupción ley 1474 de 2011, COSO ERM, Modelo Estándar de Planeación y Gestión, MECI

La Política de Administración de Riesgos establece las directrices vinculantes para todas las dependencias del Ministerio, las direcciones regionales y las áreas que ejecutan procesos tercerizados, en concordancia con la estructura ministerial definida en el Decreto 1075 de 2024. Estas políticas son de obligatorio cumplimiento y su implementación debe ser supervisada y documentada por todos los servidores públicos, contratistas y terceros que participen en los procesos institucionales, garantizando así una gestión integral y estandarizada de los riesgos en todos los niveles de la organización.

6.2.4 Política Anticorrupción

El Ministerio de Igualdad y Equidad es una entidad alineada con el Gobierno Nacional frente a la lucha contra la corrupción. Por tanto, sus servidores públicos, contratistas y proveedores debemos ser personas íntegras en nuestro actuar y proceder, honestas y transparentes, nuestra posición debe ser abiertamente en contra de cualquier conducta irregular, y nuestra actitud, la de denunciar ante las autoridades correspondientes cuando se evidencie alguna de ellas

6.2.5 Política de conflicto de interés

Los funcionarios del Ministerio de Igualdad y Equidad deberán declararse impedidos para actuar en un asunto cuando se tenga interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil. Igualmente deberá declararse impedido cuando el interés general, propio de la función pública, entre en conflicto con su interés particular y directo. La política de conflicto de interés se encuentra alineada con nuestro Código de Ética, el cual contiene las directrices comportamentales aplicables a todos los funcionarios de la entidad.

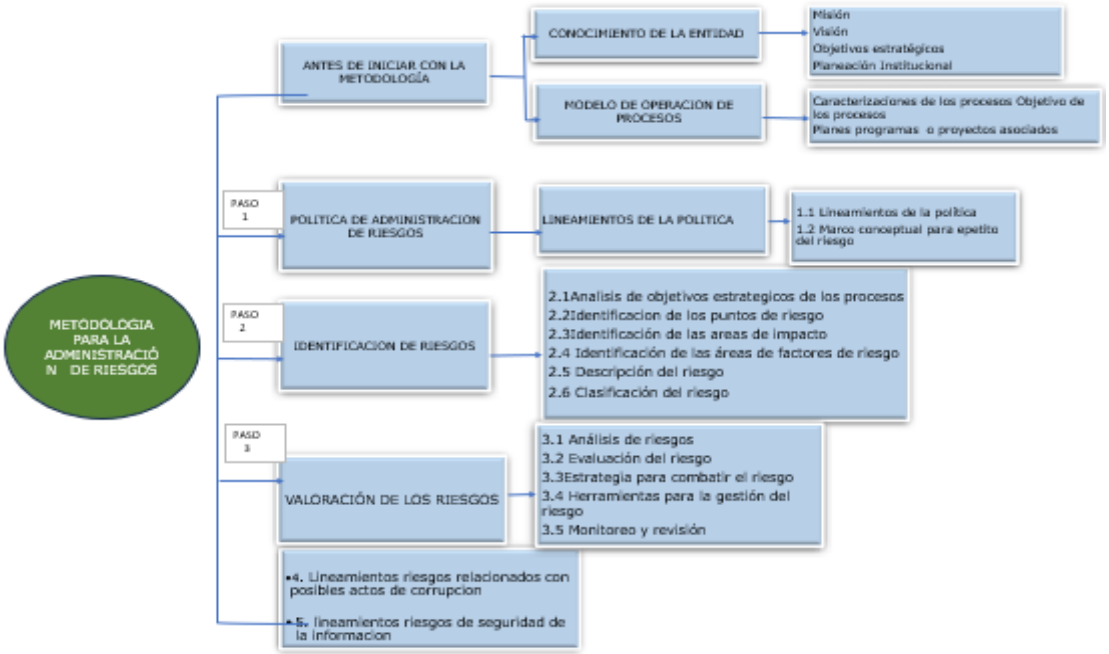
7. PROCESO DE GESTIÓN DE RIESGOS

7.1 Metodología para la Gestión de Riesgos

El Ministerio de igualdad y Equidad para la adecuada administración de riesgos adopta la metodología establecida por el DAFP, en la Guía para la Administración del Riesgo y Diseño de controles en entidades públicas-V.6-2022 del Departamento Administrativo de LA Función Pública (DAFP).

7.2 Metodología la Gestión de riegos de gestión, fiscal y corrupción

ESQUEMA 1 METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

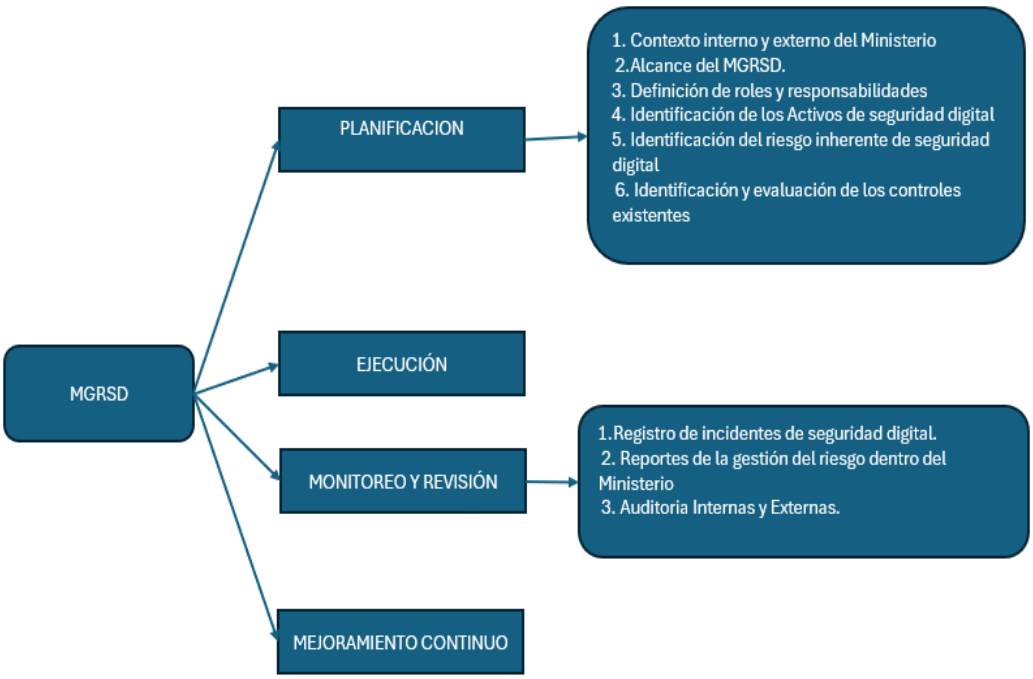


Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

7.3 Esquema para la Gestión de riesgos Digitales

La metodología para la gestión de los riesgos de Seguridad Digital se basa en la metodología establecida en el Modelo de Seguridad y Privacidad de la Información (MSPI) del DAFP (Anexo No.4**)** y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

ESQUEMA 2 ESQUEMA PARA LA GESTIÓN DE RIESGOS DIGITALES



Fuente: Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.

8. HERRAMIENTA PARA LA GESTIÓN DE RIESGOS

Ministerio de Igualdad y Equidad adopta metodología suministrada por el DAFP de conformidad con el esquema para la gestión de riesgos.

De acuerdo con lo anterior, el formato de mapa de riesgos adoptado por la entidad se encuentra controlado con el formato OAP-EE-FO-008, para la identificación; análisis; evaluación de riesgos y valoración de controles; evaluación del riesgo residual; planes de manejo con sus respectivos campos, para los riesgos de gestión, fiscal y de corrupción.

Para la gestión de los riesgos de Seguridad Digital-RSD, se estructuró la matriz para la identificación y el análisis de los riesgos inherentes; valoración de los controles y planes de manejo con sus respectivos campos con el formato OAP-EE-FO-008, bajo los parámetros de la Guía de Administración de Riesgos del DAFP y la guía Modelo de Seguridad y Privacidad de la Información -MSPI del DAFP (Anexo No.4**).**

Los formatos para la gestión de riesgos se deben diligenciar acorde con el instructivo que contiene cada formato.

8.1 Clases de Mapas

8.1.1 El mapa de riesgo por procesos OAP-EEFO-009 estará bajo la responsabilidad de cada uno de los líderes, el cual será consolidado por la Oficina de Planeación y estará conformado por los riesgos de gestión, fiscales y de corrupción de cada proceso.

8.1.2 El mapa de riesgos de Seguridad Digital OAP-EE-FO-10 estará bajo la responsabilidad del encargado de seguridad digital, será consolidado por la Oficina de Tecnologías de la Información y publicado en la intranet, por la Oficina de Planeación. Este mapa estará conformado por los riesgos de seguridad digital calificados en zona alta y extrema.

8.1.3 El mapa de riesgos Institucional OAP-EE-FO-009 es consolidado por la Oficina de Planeación y estará conformado por los riesgos residuales, que se encuentren en una zona de riesgo, moderada, alta o extrema de los riesgos de gestión, fiscales y de corrupción.

El mapa de riesgo Institucional recopila los planes de manejo de los riesgos de cada proceso y los cuales son susceptibles de seguimiento por parte de la Oficina de Planeación y de Control Interno, y presenta el resultado del monitoreo y seguimiento periódicos que se realice a los riesgos de proceso.

La Oficina de Planeación, publicará los mapas de riesgos de proceso, de Seguridad Digital, e institucional, en el repositorio KOFAN en el enlace del MIPG y el mapa de riesgos de corrupción se publicará en la página web de la Entidad, en el enlace de transparencia, de acuerdo con lo establecido en la Ley 1712 de 2014 y el Decreto 103 de 2015 y la Ley 1474 de 2011.

8.2 Importancia de la Gestión de Riesgos

- Permite identificar de manera oportuna los eventos potenciales tanto internos como externos que puedan afectar el cumplimiento de los objetivos y misión institucional.
- Evita que los eventos negativos, lesionen la imagen institucional, entorpezcan la operación, el cumplimiento de los objetivos estratégicos y metas institucionales o que afecten la prestación de los servicios.
- Permite, controlar y dar tratamiento prioritario a los riesgos de gestión y de seguridad digital de mayor incidencia y los relacionados con los riesgos de corrupción.
- Potencializa los eventos positivos, para que permitan minimizar el impacto de los posibles eventos negativos en la gestión de los riesgos.
- Identifica, disuade y detecta posibles fraudes que puedan afectar la adecuada gestión de la Entidad.
- Incrementa la confianza de todos los procesos del Ministerio en el uso del entorno digital.

8.3 Tolerancia de los riesgos

De acuerdo con la calificación de los riesgos residuales (riesgos después de controles), El Ministerio de Igualdad y Equidad establece la tolerancia y niveles de aceptación para cada uno y el plan de manejo o tratamiento de los riesgos, aplicables para los riesgos de gestión, fiscales, corrupción y los de seguridad digital.

Riesgos de Corrupción y fiscales. Para los riesgos de corrupción, sólo se tendrán dos clases de niveles de aceptación:

Evitar o reducir el riesgo. Estos niveles de aceptación, independiente de la calificación de los riesgos residuales.

Los riesgos de Corrupción y fiscales no admiten aceptación, compartir o transferir el riesgo y siempre generan tratamiento.

8.4 Niveles de aceptación al riesgo

Los niveles de aceptación del riesgo se determinan como resultado de la valoración de la probabilidad de ocurrencia del riesgo y de la magnitud del impacto al

momento de evaluar su materialización. Los riesgos de gestión inherentes, ubicados en la zona de riesgos "baja" pueden ser aceptados y por lo tanto no es necesario establecer controles. Los riesgos de corrupción son los únicos que son inaceptables en todo sentido, por tanto, deben tener controles permanentes y realizar su seguimiento.

El mapa de calor de riesgos permite visualizar los riesgos de gestión en las zonas de riesgos definidas (Baja, Moderada, Alta, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a buscar o retener (apetito del riesgo) en función del impacto de estos en la Unidad. Los riesgos que se encuentren en zona baja se aceptan, aunque representan una menor probabilidad e impacto para el Ministerio de Igualdad y Equidad, requieren un seguimiento estructurado que garantice que se mantengan en este nivel. Su monitoreo, si bien puede ser menos intensivo que el de riesgos en zonas más altas, debe ser sistemático y documentado.

Deberá ser:

- Monitoreo trimestral por primera línea
- Revisión semestral por segunda línea
- Evaluación semestral por control interno
- Actualización de valoración cuando se requiera
- Verificación ante cambios significativos
- Mantención del nivel de riesgo

El mapa de calor de riesgos permite visualizar los riesgos de seguridad digital en las zonas de riesgos definidas (Bajo, Moderado, Alto, Extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención; estableciendo un plan de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociado a los activos de información sin importar el nivel de criticidad que tienen para la entidad. Los riesgos de seguridad digital que se encuentren en las zonas Bajo se aceptan aunque representan una menor probabilidad e impacto, requieren el mimo seguimiento que los riesgos de gestión de zona baja:

- Monitoreo trimestral por primera línea

- Revisión semestral por segunda línea
- Evaluación semestral por control interno
- Actualización de valoración cuando se requiera
- Verificación ante cambios significativos
- Mantención del nivel de riesgo

La Línea Estratégica, debe asegurar una gestión adecuada de los riesgos ubicados en zona baja, garantizando que su tratamiento sea proporcional y eficiente, sin descuidar su monitoreo y control, teniendo en cuenta los siguientes aspectos:

- Validación semestral de informes consolidados
- Evaluación de estrategia de tratamiento
- Toma de decisiones sobre ajustes requeridos
- Definir información requerida
- Determinar indicadores clave
- Aprobar metodología de seguimiento
- Establecer canales de comunicación
- Mantener supervisión adecuada

Los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento. Los riesgos que se encuentran en las zonas más altas son los que se priorizan orientando los esfuerzos y acciones para mejorar su administración de riesgos.

Riesgos de Corrupción y fiscales. Para los riesgos de corrupción, sólo se tendrán dos clases de niveles de aceptación:

- **Evitar o reducir el riesgo.** Estos niveles de aceptación, independiente de la calificación de los riesgos residuales.

Los riesgos de Corrupción y fiscales no admiten aceptación, compartir o transferir el riesgo y siempre generan tratamiento**.**

8.5 Riesgos de gestión y de seguridad digital

Asumir (aceptar) la presencia de un riesgo mínimo o residual después de que el riesgo se ha reducido.

Medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de protección). Se puede conseguir mediante la optimización de los procedimientos y la implementación de controles preventivos.

Medida encaminada a eliminar la actividad que genera el riesgo (probabilidad y/o impacto), previniendo su materialización.

Medidas que reducen el efecto de un riesgo, a través del traspaso de las pérdidas a otras organizaciones. Y se establecen planes de contingencia en caso de materialización.

8.6 Riesgos de Corrupción o fiscales:

La lucha contra la corrupción en el Ministerio de Igualdad y Equidad constituye un pilar fundamental para garantizar la efectiva implementación de programas y proyectos dirigidos a los sujetos de especial protección constitucional y territorios históricamente excluidos. Siendo un ministerio de reciente creación, resulta imperativo establecer desde su inicio mecanismos robustos de prevención, detección y sanción de actos de corrupción que puedan afectar los recursos destinados a reducir las brechas

de desigualdad en Colombia. La implementación de medidas anticorrupción no solo fortalece la transparencia, sino que asegura que los beneficios lleguen efectivamente a las poblaciones más vulnerables, contribuyendo así al cumplimiento de la misión institucional de avanzar en la garantía del derecho a la igualdad concentran y la equidad para todos los colombianos, con especial énfasis en aquellos que han enfrentado barreras históricas de discriminación y exclusión.

Teniendo en cuenta el Plan Estratégico de la entidad encontramos varios puntos que presentan mayor susceptibilidad a riesgos de corrupción entre ellos:

Asignación y Distribución de Recursos:

- La gestión de ayudas y subvenciones para poblaciones vulnerables.
- La distribución de recursos para proyectos comunitarios.
- El manejo de presupuestos para infraestructura en territorios excluidos
- La asignación de recursos para iniciativas económicas y productivas.

Contratación y Alianzas:

- Los procesos de contratación para la infraestructura destinada a cerrar brechas territoriales
- La selección de socios para las "Alianzas Públicas Populares, Comunitarias y Solidarias"
- La contratación de servicios para los Espacios para la Juntanza

Gestión de Programas Sociales:

- La selección de beneficiarios para programas de apoyo.
- La implementación de iniciativas económicas y productivas.
- La distribución de beneficios en territorios marginados

Coordinación Territorial:

- La articulación con entidades territoriales
- La focalización de programas en territorios específicos.

- La implementación de proyectos en zonas marginadas.

Procesos Administrativos:

- La supervisión de contratos y convenios.

La susceptibilidad a la corrupción en estos procesos se incrementa debido a:

- El manejo de recursos significativos
- La interacción con poblaciones vulnerables
- La dispersión geográfica de las intervenciones.
- La complejidad en la verificación y seguimiento
- La discrecionalidad en la toma de decisiones.
- La presión por resultados rápidos en la implementación de programas

es fundamental establecer un riguroso sistema de tratamiento y seguimiento a los riesgos de corrupción, el éxito en la prevención de la corrupción dependerá de la rigurosidad en la implementación y seguimiento de estas medidas, así como de la participación activa de todos los actores involucrados.
El control y seguimiento será el definido en el numeral 11.1 Monitoreo de los riesgos y controles.

8.6.1 Estrategias para Minimizar Riesgos de Corrupción en Programas y Proyectos

Para minimizar los riesgos de corrupción en los programas y proyectos del Ministerio de Igualdad y Equidad, se propone implementar un sistema integral que combina transparencia activa, gestión digital y control social. Este sistema incluye la publicación en tiempo real de la ejecución presupuestal, plataformas digitales para seguimiento de beneficiarios con verificaciones, veedurías ciudadanas con enfoque territorial y poblacional, y mecanismos de control preventivo basados en análisis predictivo de riesgos. Se fortalece con la participación comunitaria a través de comités locales de vigilancia, rendición de cuentas programática mediante tableros de control público, articulación con órganos de control y capacitación especializada del personal interno. Todas estas medidas se implementan bajo los enfoques diferenciales del Ministerio, asegurando que la lucha anticorrupción sea efectiva y culturalmente pertinente.

- Para los riesgos de corrupción, sólo se tendrán dos clases de niveles de aceptación:

1.Evitar o reducir el riesgo. Estos niveles de aceptación, independiente de la calificación de los riesgos residuales.

2.Los riesgos de Corrupción y fiscales no admiten aceptación, compartir o transferir el riesgo y siempre generan tratamiento.

8.7 Tratamiento o manejo de los riesgos.

A continuación, se presenta el manejo o tratamiento de los riesgos para el Ministerio, de acuerdo con la calificación después de controles (riesgos residuales), los cuales se califican en zona de riesgo baja, zona de riesgo moderado, zonal de riesgo alta y zona de riesgo extrema. (La metodología para la valoración de los riesgos, se detalla en el numeral 10.2 del presente documento).

Para los riesgos de Seguridad Digital, de acuerdo con la zona que se califique el riesgo, se establece los niveles y el tratamiento que se debe dar, con el fin de evitar su materialización, reducir la zona del riesgo o eliminar el riesgo.

Se debe realizar en primera medida la identificación de los riesgos de seguridad digital para luego definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los niveles establecidos.

El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales, El Ministerio establece como prioridad el tratamiento de los riesgos de seguridad digital ubicados en las zonas de riesgo altas y extremas.

Calificación del Riesgo	(Niveles de aceptación)	Plan de Manejo o Tratamiento del Riesgo
ZONA BAJA	**ASUMIR O ACEPTAR EL RIESGO**	Riesgos inherentes, no se requiere adoptar medidas para su tratamiento. Realizar monitoreo periódico (trimestral) a los riesgos para que permanezcan en zona baja o se permita eliminar el riesgo.
ZONA MODERADA	**REDUCIR EL RIESGO**	Establecer acciones, medidas que permitan reducir la probabilidad y/o el impacto del riesgo. Monitoreos periódicos, mínimo cada trimestre a los riesgos y

Calificación del Riesgo	(Niveles de aceptación)	Plan de Manejo o Tratamiento del Riesgo
		controles. Optimizar los procedimientos de seguridad digital establecidos.
ZONA ALTA	**EVITAR EL RIESGO**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. Monitoreo bimensual a los riesgos y controles. Realizar mantenimiento preventivo a la infraestructura tecnológica.
ZONA EXTREMA	**EVITAR EL RIESGO COMPARTIR O TRANSFERIR EL RIESGO**	Monitoreo mensual a los controles y riesgos y establecer planes de contingencia en caso de materialización. Realizar Contratos de Mantenimiento correctivo, y de soporte sobre la plataforma tecnológica con proveedores. Establecer Contratos de seguro.

TABLA 1 TRATAMIENTO DE LOS RIESGOS DE GESTIÓN
Fuete: Elaboración Propia

Tratamiento riesgos de corrupción y fiscales

Calificación del Riesgo	(Niveles de aceptación)	Plan de Manejo o Tratamiento del Riesgo
ZONA BAJA		Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad de ocurrencia. Monitoreos periódicos, mínimo cada trimestre a los controles y acciones.
ZONA MODERADA	**REDUCIR EL RIESGO**	
ZONA ALTA	**EVITAR EL RIESGO COMPARTIR O TRANSFERIR EL RIESGO**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando la probabilidad de ocurrencia. Monitoreos bimensuales o mensuales a los riesgos y los controles. Establecer planes de contingencia para aplicar en caso de materialización.
ZONA EXTREMA		

TABLA 2 TRATAMIENTO DE RIESGOS DE CORRUPCIÓN Y FISCALES
Fuente: Ministerio de Igualada y Equidad

8.8 Tratamiento a los riesgos materializados-.

Ante la materialización de riesgos institucionales, es fundamental ejecutar un protocolo estructurado que inicie con la activación inmediata del las tres líneas de Defensa para documentar y contener el incidente, seguido de una evaluación

exhaustiva del impacto que permita cuantificar daños y revisar la efectividad de los controles existentes. Posteriormente, se debe implementar un plan de mitigación con acciones correctivas específicas, responsables y recursos asignados, para luego proceder con la fase de recuperación que incluye la ejecución del plan de continuidad y el restablecimiento de operaciones normales. Todo el proceso debe ser monitoreado continuamente, documentado detalladamente y utilizado como insumo para la mejora continua del sistema de gestión de riesgos, actualizando controles, políticas y procedimientos según las lecciones aprendidas.

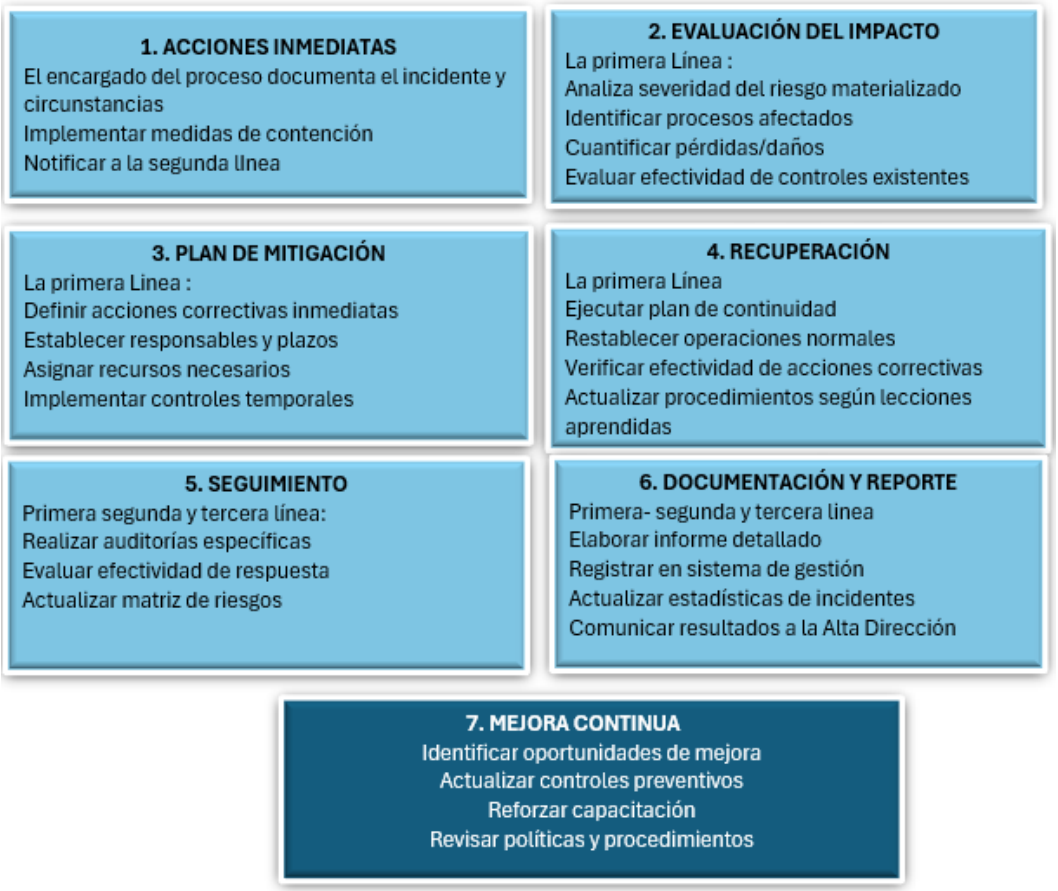


TABLA 3 TRATAMIENTO DE RIESGOS MATERIALIZADOS
Fuente: Ministerio de Igualada y Equidad

En respuesta, la Alta Dirección debe tomar decisiones inmediatas sobre recursos extraordinarios, modificaciones a procesos y planes de comunicación, además de establecer mecanismos de seguimiento como comités y reportes periódicos. Es fundamental que la Alta Dirección autorice e implemente mejoras sistémicas, incluyendo actualizaciones de políticas, nuevos controles y asignación de

presupuesto para fortalecimiento institucional, asegurando así un ciclo efectivo de mejora continua en la gestión de riesgos.

9. ROLES Y RESPONSABILIDADES

El Ministerio de Igualdad y Equidad , estructura los criterios para la adecuada toma de decisiones respecto al tratamiento de los riesgos y sus efectos al interior de la entidad, por lo tanto, la implementación y mantenimiento de la Política de Administración de Riesgos, la metodología y tratamiento de los mismos, debe ser establecida por la Dirección con el apoyo del equipo directivo, el equipo operativo (líderes de proceso y gestores del Sistema de Gestión) y debe ser interiorizada por todos los servidores públicos y contratistas de la Entidad, responsables del desarrollo de actividades de los diferentes procesos.

Para la adecuada gestión de los riesgos de gestión, corrupción y de seguridad digital, el Ministerio de Igualdad y Equidad define los niveles de responsabilidad y autoridad acorde con las líneas de defensa definidas en la Entidad, con el fin implementar, coordinar, revisar, monitorear, hacer seguimiento y evaluar los riesgos inherentes a cada proceso.

Líneas de Defensa:

Las Líneas de Defensa proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados. Este modelo proporciona una mirada a las operaciones, ayudando a asegurar el éxito continuo de las iniciativas de gestión del riesgo, y este modelo es apropiado para cualquier entidad – independientemente de su tamaño o complejidad" (IIA 2013:2). Las responsabilidades de la gestión de riesgos y del control están distribuidas en varias áreas y no se concentran en las oficinas de control interno; de allí que deban ser coordinadas cuidadosamente para asegurar que los controles operen. La adaptación este enfoque se presenta en la siguiente gráfica.

Líneas de defensa:

LINEA ESTRATEGICA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
ALTA DIRECCIÓN Y COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO **Su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos**	Definir y aprobar la Política de Administración de Riesgos de la del Ministerio de Igualdad y Equidad, en el marco del Comité Institucional de Coordinación de Control Interno y el liderazgo del Representante Legal. Evaluar la Política de Administración de Riesgos, la cual debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo. Establecer los lineamientos y metodología para el tratamiento, manejo y seguimiento de los riesgos, incluyendo los riesgos de gestión, corrupción y de seguridad digital, que puedan afectar el logro de los objetivos institucionales. Establecer los roles y las responsabilidades frente a la Gestión de Riesgos de la Entidad incluyendo el responsable de Seguridad de la Información para la efectiva administración de los Riesgos de SD. Revisar y analizar los cambios en el "Direccionamiento estratégico", para la identificación de nuevos riesgos o la modificación de los que ya se tienen identificados, considerando los cambios en el entorno y los riesgos emergentes, que puedan afectar el cumplimiento de los objetivos estratégicos. Analizar los resultados del seguimiento de los riesgos estratégicos y de mayor impacto, para tomar acciones estratégicas que permitan mitigar la ocurrencia de los riesgos. Revisar en forma periódica el resultado del cumplimiento de los objetivos estratégicos y metas institucionales y de procesos, así como de los indicadores, para identificar posibles riesgos que se están materializando por no cumplimiento de estos.

TABLA 4 ROLES Y RESPONSABILIDADES LÍNEA ESTRATÉGICA

Fuente: Manual Operativo MIPG V.4 DAFP- Guía Administración Riesgos V.6 DAFP

PRIMERA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad. **Rol principal: diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la entidad.**	Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro. establecimiento de actividades de control.
	Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos

TABLA 5 ROLES Y RESPONSABILIDADES PRIMERA LÍNEA DE DEFENSA
FUENTE: MANUAL OPERATIVO MIPG V.4 DAFP- GUÍA ADMINISTRACIÓN RIESGOS V.6 DAFP

SEGUNDA LÍNEA DE DEFENSA ROLES	RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS
Conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia**)**. Quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección	Asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos. Hacer seguimiento a las actividades de manejo para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. Supervisores: alertar sobre la posible materialización de los riesgos identificados en la ejecución de los contratos
OFICINA DE PLANEACIÓN	Asesorar a la línea estratégica en el análisis del contexto interno y externo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. Apoyar a la Alta Dirección en la estructuración y definición de la Política de Administración de riesgos Del Ministerio , para presentarla al Comité Institucional de coordinación de Control Interno- CICCI. Hacer seguimiento periódico a los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles. Consolidar el Mapa de riesgos Institucional con los riesgos de corrupción y fraude y los riesgos de gestión calificados en zona moderada, alta y extrema. Realizar la difusión y asesoría de la metodología para la gestión de riesgos adoptada por El Ministerio Orientar y acompañar a los líderes de procesos en la gestión de riegos (gestión y corrupción) en cada una de sus etapas (Identificación, análisis, evaluación, establecimiento de controles y planes de manejo). Fomentar la administración del riesgo como una actividad inherente al proceso de Planeación Estratégica, trabajando en forma coordinada y armónica con la Oficina de Comunicaciones y el Grupo Interno de Control Interno. Revisar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisar que la implementación de los planes de manejo de los riesgos sea eficaz.

TABLA 6 ROLES Y RESPONSABILIDADES DE LA SEGUNDA LÍNEA DE DEFENSA0

Fuente: Manual Operativo MIPG V.4 DAFP- Guía Administración Riesgos V.6 DAFP

TERCERA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO	Evaluar de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa. A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos. Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Asesorar proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. Comunicar a la Alta Dirección, sobre el resultado de la evaluación a la gestión de riesgos y los posibles cambios e impactos, en el cumplimiento de los objetivos institucionales. (riesgos de corrupción y posibles fraudes) Proporcionar información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. Le corresponde al GIT de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la Entidad, a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Evaluar la eficacia de la gestión de riesgos en la Entidad, el diseño y efectividad de los controles e informar a la Dirección sobre la efectividad de estos.

TABLA 7 OPERATIVIDAD DE LA TERCERA LÍNEA DE DEFENSA
Fuente: Manual Operativo MIPG V.4 DAFP- Guía Administración Riesgos V.6 DAFP

La periodicidad para el monitoreo de los riesgos y seguimiento de los controles se establece en el **11.2.2,** del presente documento, de acuerdo con la calificación de los riesgos residuales.

Además de las líneas de defensa y las responsabilidades asignadas para la Administración de Riesgos, a continuación, se presentan las responsabilidades establecidas en el Modelo de Seguridad y Privacidad de la Información MSPI- dadas en la Estrategia de Gobierno Digital del MINTIC**,** al responsable de Seguridad

Digital, quien debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica[1].

El responsable de Seguridad Digital será quien tenga las siguientes responsabilidades respecto a la Gestión de Riesgos de Seguridad Digital (GRSDI):

ROLES Y RESPONSABILIDADES DE SEGURIDAD DIGITAL	
PRIMERA LÍNEA DE DEFENSA **Responsable de la seguridad Digital**	Definir el procedimiento para la Identificación y Valoración de Activos.
	Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
	Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
	Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
	Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
SEGUNDA LÍNEA DE DEFENSA **Oficial de seguridad**	Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
	Definir el procedimiento o metodología para la Identificación y Valoración de Activos
	Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.
	Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
	Supervisar la respuesta a incidentes, así como l investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
	Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
	Realizar y/o supervisar pruebas de vulnerabilidades sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información

TABLA 85 RESPONSABILIDADES, RIESGOS, SEGURIDAD DIGITAL
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

10. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DEL MINISTERIO DE IGUALDAD Y EQUIDAD

El Ministerio de Igualdad y Equidad para la adecuada administración de riesgos adopta la metodología establecida por el DAFP, en la Guía para la Administración del Riesgo y Diseño de controles en entidades públicas Versión 6 de 2022 del DAFP,

[1] Anexo 4. Lineamientos para la gestión de riesgos de SD, en entidades públicas, MINTIC-2018

el Modelo de Seguridad y Privacidad de la Información -MSPI del DAFP (Anexo No.4**).**

10.1 Identificación y análisis de riesgos.

La identificación de los riesgos tiene como objetivo, identificar las fuentes, eventos de riesgos, sus causas y consecuencias, que puedan incidir en la consecución de los objetivos estratégicos y objetivos de los procesos.

Esta etapa, inicia con el establecimiento del contexto estratégico de la entidad y de proceso, una vez se establece, se inicia con la construcción de los riesgos por procesos, sus causas y consecuencias.

10.1.1 Contexto estratégico.

La identificación del riesgo debe ser un proceso permanente, se parte del conocimiento estratégico de la Entidad, la misión, la visión y los objetivos estratégicos, a partir de los cuales se identifican los factores o eventos internos o externos, que pueden ocasionar riesgos que afecten el logro de los objetivos institucionales.

Para la identificación de los riesgos de proceso, se pueden involucrar datos históricos, análisis teóricos, opiniones informales y expertas, planeación institucional, mapa de procesos, caracterizaciones, procedimientos, entre otros, a fin de conocer con claridad el entorno, para establecer los eventos que pueden tener incidencia en el cumplimiento de los objetivos del proceso y proyectos.

Contexto externo: Este inicia con el análisis y establecimiento de los factores externos que puedan afectar a la Entidad para el cumplimiento de la misión y objetivos estratégicos.

Contexto interno: Se tiene en cuenta las condiciones internas que puedan afectar el cumplimiento de la misión, objetivos estratégicos, procesos de la Entidad (Estratégicos, Misionales, Apoyo y Evaluación), cumplimiento de procedimientos.

10.1.2 Identificación de los puntos críticos

Para la identificación de los riesgos de proceso, se debe tener en cuenta 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[2].

Es importante que se analice la secuencia de los procesos y la cadena de valor, lo cual permite identificar los puntos críticos y el establecimiento de las actividades que pueden generar riesgo para el cumplimiento de los objetivos de los procesos de la Entidad. (mapa de procesos)

10.1.3 Identificación de las áreas de impacto.

De conformidad con la metodología establecida por el DAFP, se debe identificar las áreas de impacto, estas son: "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." [3]

10.1.4 Identificación de las áreas de factores de riesgos.

Estas hacen referencia a la identificación de las fuentes generadoras de riesgos que pueda tener la Entidad, a nivel interno y externo.

FACTOR	DEFINICIÓN	DESCRIPCIÓN
PROCESO	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización	Falta de procedimientos Errores de registro, 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 de activos Posibles comportamientos no éticos de los empleados Fraude interno (corrupción, soborno
TECNOLOGÍA	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos Caída de aplicaciones Caída de redes Errores en programas
INFRAESTRUCTURA	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes Incendios

[2] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6
[3] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6

FACTOR	DEFINICIÓN	DESCRIPCIÓN
		Inundaciones Daños a activos fijos
EVENTOS EXTERNOS	Situaciones externas que afectan la entidad.	Suplantación de identidad Asalto a la oficina Atentados, vandalismo, orden público Fuerza mayor o caso fortuito

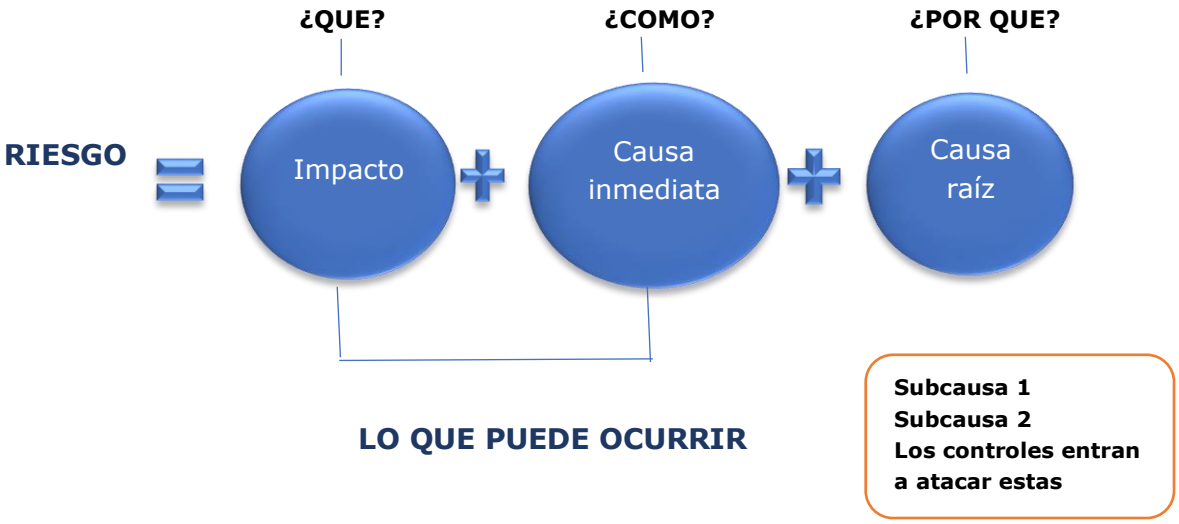
TABLA 9 AREAS DE FACTORES DE RIESGO
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

10.1.5 Descripción del riesgo de gestión

Para la describir o redactar el riesgo en forma adecuada, de tal forma que permita una interpretación adecuada, se debe tener en cuenta:

Iniciar con la palabra **"POSIBILIDAD"** y seguidamente, analizar los siguientes aspectos:

ESQUEMA 3 DESCRIPCIÓN DEL RIESGO



Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Es necesario identificar la causa inmediata (cómo) y la causa raíz (por qué), con el fin de que el riesgo quede bien identificado y su descripción evite interpretaciones subjetivas.

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata**: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz**: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo.

Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Premisas para tener en cuenta en la redacción del riesgo:

- **No** describir como riesgos omisiones ni desviaciones del control.
- **No** describir causas como riesgos
- **No** describir riesgos como la negación de un control.
- **No** existen riesgos transversales, lo que pueden existir son causas transversales

10.1.6 Clasificación y factores de Riesgo.

Para establecer una adecuada clasificación de los riesgos identificados se tienen la siguiente tipología, asociados a los procesos así[4]:

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

Fraude externo: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude interno: Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

[4] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6

Fallas tecnológicas: Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Relaciones laborales: Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

Usuarios, productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos fijos/eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Para la identificación de los riesgos, se hace necesario tener en cuenta los factores de riesgos:

FACTORES DE RIESGO	
CLASIFICACIÓN	**FACTORES DE RIESGOS**
Ejecución y administración de procesos	Procesos
Fraude externo	Eventos externos
Fraude interno	Talento Humano
Fallas tecnológicas	Tecnología
Relaciones laborales	Se asocian a varios factores
Usuarios, productos y prácticas	Se asocian a varios factores
Daños a activos fijos/eventos externos	Infraestructura- Evento externo

TABLA 10 FACTORES DE RIESGOS
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

10.2 Valoración de los Riesgos

La valoración de riesgos consiste en establecer la probabilidad de ocurrencia del riesgo y nivel de consecuencia del impacto, con el fin de estimar la zona de riesgo inicial- RIESGO INHERENTE[5].

Los elementos que se deben tener en cuenta para realizar la valoración son:

El análisis del riesgo: Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial o riesgo inherente.

Evaluación de riesgos: Se busca confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final o riesgo residual.

10.2.1 Análisis de riesgos.

La construcción de los riesgos se realiza a partir de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

10.2.1.1 Determinación de la probabilidad.

La probabilidad o posibilidad de ocurrencia del riesgo, está asociada a la exposición del riesgo del proceso que se encuentra en análisis.

- ***La probabilidad inherente: es el número de veces o frecuencia que se repite la actividad en un año***
- ***La exposición al riesgo estará asociada al proceso o actividad que se esté analizando***

Criterios para definir el nivel de probabilidad

Las tablas de calificación del impacto definidas para los Riesgos de Gestión, Corrupción y Seguridad Digital se definen así:

[5] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6

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

TABLA 11 CRITERIOS PARA DEFINIR EL NIVEL DE PROBABILIDAD
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

10.2.1.2 Determinación del Impacto.

Para establecer el impacto de los riesgos identificados, se toman las variables de

IMPACTO ECONÓMICO y REPUTACIONAL, lo que permite que la evaluación del riesgo sea más objetiva.

En el caso de que se presenten ambas variables, se toma la que presente el mayor nivel más alto.

IMPACTO			
Nivel	**% Impacto**	**Afectación económica**	**Reputacional**
Leve	**20%**	Menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	**40%**	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado	**60%**	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.

IMPACTO			
Nivel	**% Impacto**	**Afectación económica**	**Reputacional**
Mayor	**80%**	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico	**100%**	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

TABLA 12 CRITERIOS PARA DEFINIR EL NIVEL DE IMPACTO
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

- ***El líder del proceso será quien determine los criterios de probabilidad e impacta para el análisis del riesgo, que es quien conoce el proceso.***

10.2.2 Evaluación de los Riesgos

A partir del análisis de probabilidad e impacto, se establece la zona inicial que queda ubicado el riesgo inherente, en la tabla de calor.

Esta se determina mediante la combinación de la probabilidad y el impacto así:

%	MATRIZ CALIFICACIÓN DE RIESGOS IMPACTO					
100%	Muy alta	ALTA	ALTA	ALTA	ALTA	EXTREMA
80%	Alta	MODERADA	MODERADA	ALTA	ALTA	EXTREMA
60%	Media	MODERADA	MODERADA	MODERADO	ALTA	EXTREMA
40%	Baja	BAJA	MODERADA	MODERADO	ALTA	EXTREMA
20%	Muy baja	BAJA	BAJA	MODERADO	ALTA	EXTREMA
	PROBABILIDAD	LEVE 20%	MENOR 40%	MODERADO 60%	MAYOR 80%	CATASTROFICO 100%
		IMPACTO				

TABLA 13 EVALUACIÓN DE LOS RIESGOS
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Como resultado de la evaluación los riesgos inherentes, se pueden ubicar en las siguientes zonas:

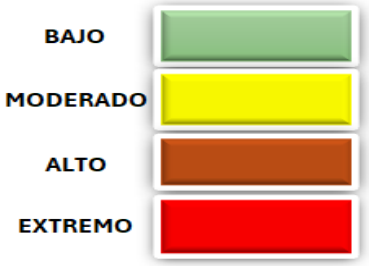


TABLA 14 ZONAS DE RIESGOS
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Una vez se obtiene la calificación y zona donde queda ubicado el riesgo inherente, se continúa con el establecimiento de controles y la valoración de estos, permitiendo establecer el riesgo residual (después de controles).

10.3 Valoración de los Controles.

El control se define como la medida que permite reducir o mitigar el riesgo, para lo cual se debe tener en cuenta[6]:

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

  De acuerdo con la tipología de los controles se clasifican en:

  Controles Preventivos: Son los que actúan en la entrada del proceso y antes de que se realice la actividad que origina el riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

  Controles Detectivos: Son los que actúan durante la ejecución de la actividad. Detectan el riesgo, pero generan reproceso.

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

[6] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6

De acuerdo con la forma como se ejecutan los controles, se clasifican en:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Las actividades de control tienen como fin:

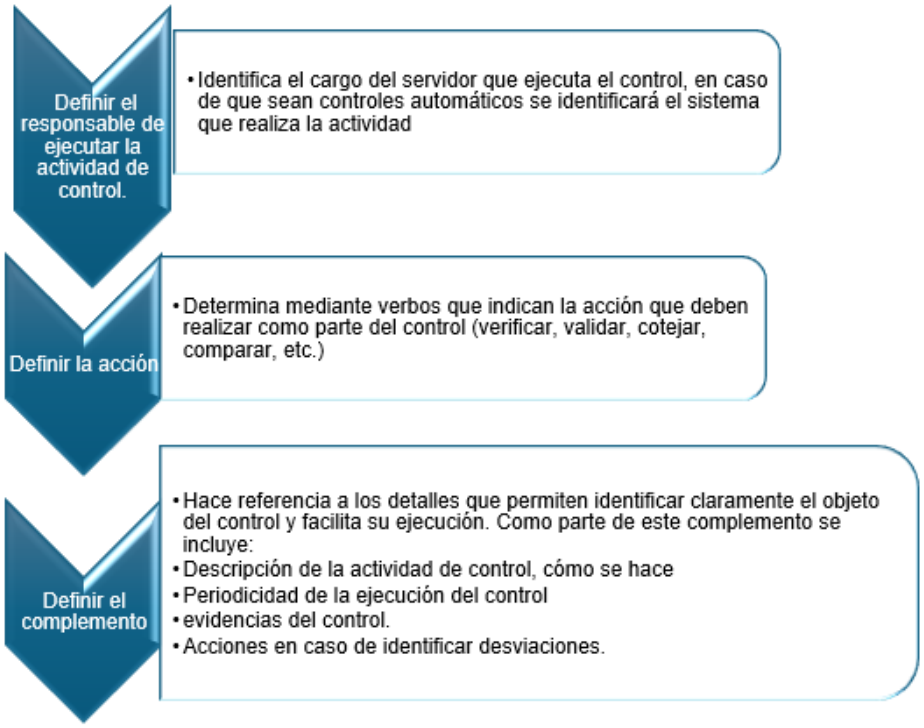
TIPO DE CONTROL	RESULTADO	ETAPAS DEL PROCESO
Controles Preventivos	Va a las causas del riesgo Atacan la probabilidad de ocurrencia del riesgo	Entradas
Controles Detectivos	Detecta que algo ocurre y devuelve el proceso a los controles preventivos Atacan la probabilidad de ocurrencia del riesgo	Ejecución de actividades
Controles Correctivos	Atacan el impacto frente a la Materialización del riesgo	Salidas

TABLA 15 ACTIVIDADES DE CONTROL
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

10.3.1 Estructura de los Controles

El DAFP, en la Guía de Administración de Riesgos y diseño de controles, establece la siguiente estructura para la valoración de los controles, la cual parte de la metodología anterior, así:

ESQUEMA 4 ESTRUCTURA DE CONTROLES



Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

- La identificación de los controles se debe realizar para cada riesgo.
- Los responsables de implementar monitorear los controles de los riesgos ***son los líderes de proceso y los responsables de su ejecución.***

10.3.2 Diseño de los Controles

A continuación, se presenta la metodología, para el diseño, análisis y evaluación de los controles asociados a los riesgos, lo cual permitirá establecer el riesgo residual y su tratamiento.

Atributos para el diseño de los controles.

Para el diseño de los controles, se tienen en cuenta dos clases de atributos: Atributos de eficiencia y Atributos informativos.

CARACTERISTICAS			DESCRIPCION	PESO
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo,aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos.Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo,tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automáticas in la intervención de personas para su realización.	25%
		Manual	Controles que so nejecutados por una persona.,tiene implícito el error humano.	15%
VALORACIÓN DEL CONTROL				90%
Atributos de Eficiencia	Documentación	Documentaso	Controles que están documentados en el proceso,ya sea en manuales, procedimientos,flujogramas o cualquier otro documento propio del proceso.	
		Sin Documentar	dentificaaloscontrolesquepeseaqueseejecutanenelprocesonoseencuentrandocumentadosenningúndocumentopropiodelproceso	
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad	
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	
	Eficiencia	Con registro	Elcontroldejaunregistroquepermiteevidenciarlaejecución del control-	
		Sin registro	El control no deja registro de la ejecución del control-	

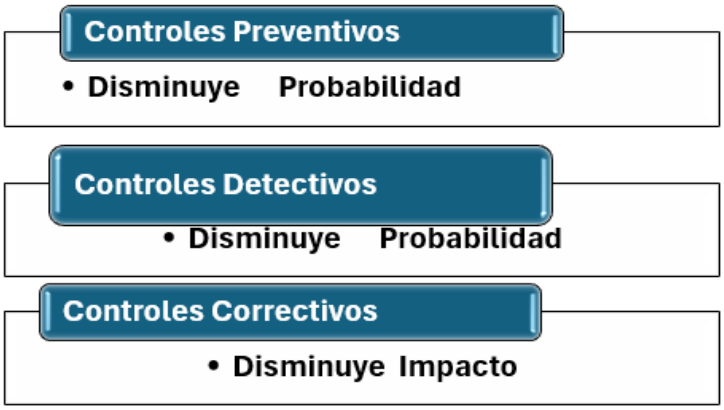
Tabla 66 ATRIBUTOS DE LOS CONTROLES

Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Los atributos de eficiencia dan una evaluación al control cuantitativa, lo cual permite determinar la efectividad del control y establecer la evaluación final del riesgo, al moverse en la matriz de calor (riesgo residual), de acuerdo con el tipo de control y disminuir la probabilidad o el impacto.

Los atributos informativos, sólo dan formalidad al control, permitiendo conocer el entorno del control de forma cualitativa, ***estos no generan calificación en la evaluación del control.***

ESQUEMA 5 IMPACTO DEL CONTROL



Fuente: Ministerio de Igualada y Equidad

Nivel de riesgo residual.

Este se obtiene de aplicar la efectividad de todos los controles al riesgo inherente.

- Para la aplicación de los controles se debe tener en cuenta que los controles 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[7].

Para la identificación, valoración de controles se cuenta con la Matriz Mapa de Riesgo OAP-EE-FO-008**,** la cual se adoptó del formato del DAFP, anexo de la Guía de Administración de Riesgos y establecimiento de controles V.6-2022.

Este formato se encuentra parametrizado y el cual genera la calificación del riesgo residual de conformidad con la clase de control, evaluación de sus atributos y generación del resultado final de acuerdo con la evaluación final de los controles que se identifiquen para cada riesgo.

[7] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6

EVALUACIÓN DEL RIESGO - VALORACIÓN DE LOS CONTROLES									EVALUACIÓN DEL RIESGO- NIVEL DEL RIESGO RESIDUAL					
			ATRIBUTOS											
No de control	Descripción del control	Afectación	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual final	%	Impacto Residual final	%	Zona Residual Final	Tratamiento
1		Probabilidad	Detectivo	Manual	30%	Sin documentar	Continua	Con registro	Baja	28%	Leve	20%	Bajo	Aceptar

Tabla 17 EVALUACIÓN DEL RIESGO

Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

10.4 Tratamiento de riesgos residuales.

El tratamiento o manejo de riesgos, es el conjunto de medidas que se toman, con el fin de tratar los riesgos y mitigar su materialización a través de la toma de medidas o acciones para su mitigación.

RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL			
CALIFICACIÓN	**POLITICA MANEJO DEL RIESGO**	**PLAN DE MANEJO**	**PLAN DE CONTINGENCIA**
Zona baja	**Asumir o aceptar el riesgo**	Riesgos inherentes, no se adoptan medidas que afecten la probabilidad o el impacto. Realizar monitoreos periódicos, semestral o trimestralmente, realizar controles para que permanezcan en zona baja.	**NA**
Zona Moderado	**Reducir el riesgo**	Establecer acciones, medidas que permitan reducir la probabilidad y/o el impacto del riesgo. Monitoreos periódicos, mínimo cada trimestre	**NA**
Zona Alta	**Evitar el riesgo**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. Monitoreo bimensual a los controles y acciones establecidas.	Es optativo establecer planes de contingencia, para aplicar en caso de que el riesgo se materialice.

RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL			
CALIFICACIÓN	**POLITICA MANEJO DEL RIESGO**	**PLAN DE MANEJO**	**PLAN DE CONTINGENCIA**
Zona Extrema	**Evitar el riesgo Compartir o transferir el riesgo**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando tanto la probabilidad y/o impacto. Monitoreo mensual a los controles y acciones establecidas.	Establecer planes de contingencia para aplicar en caso de que el riesgo se materialice.

TABLA 78 RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL
Fuente: Anexo 4 MINTIC

Con base en el **formato OAP-EE-FO-009** Mapa de Riesgos, cada líder de proceso y el gestor(es), junto con su equipo de trabajo, de acuerdo con la calificación y la zona de riesgo que haya quedado ubicado el riesgo, establecen el tratamiento para cada uno, de conformidad con las Políticas de Administración adoptadas por el Ministerio.

RIESGOS DE CORRUPCIÓN			
CALIFICACION	**POLITICA MANEJO DEL RIESGO**	**PLAN DE MANEJO**	**PLAN DE CONTINGENCIA**
Zona baja	**REDUCIR EL RIESGO**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad de ocurrencia. Monitoreos periódicos, mínimo cada trimestre a los controles y acciones.	
Zona Moderado			
Zona Alta	**EVITAR EL RIESGO**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando la probabilidad de ocurrencia. Monitoreos bimensuales o mensuales a los controles y acciones establecidas	Establecer planes de contingencia para aplicar en caso de materialización
Zona Extrema			

TABLA 19 TRATAMIENTO DE RIESGOS DE CORRUPCIÓN
Fuente: Ministerio de Igualada y Equidad

10.4.1 Planes de Manejo para mitigar los riesgos.

En el Plan de Manejo de riesgos, se establecen las acciones o medidas a seguir de acuerdo con la zona y el nivel de aceptación de cada uno y de acuerdo con la solidez de los controles, con el fin de mitigar las causas generadoras de riesgos.

Para el establecimiento de las acciones se debe tener en cuenta:

- Los riesgos de GESTIÓN que permanezcan en Zona BAJA, no se requiere establecer Planes de Manejo, se debe llevar un monitoreo periódico, para evitar su materialización
- Para los riesgos que se encuentren en ZONA MODERADA, ALTA O EXTREMA, se debe establecer acciones que permitan evitar que el riesgo se materialice.
- Los riesgos de CORRUPCIÓN, independiente de la zona donde se encuentren, se les debe establecer planes de manejo para evitar su materialización y

Planes de Contingencia:

Son planes de manejo para los riesgos que se les debe dar un tratamiento especial o se les establece generalmente, para los riesgos calificados en zona alta o extrema y se ponen en marcha, en caso de materialización del riesgo.

Este Plan de Manejo se registra en el formato OAP-EE-FO-008 Mapa de Riesgos, en el campo de PLAN DE MANEJO, el cual contiene:

- Las acciones para la mitigación de los riesgos.
- Los responsables de ejecutar las acciones
    - Las fechas de inicio y finalización de las acciones.
    - Los seguimientos a las mismas
    - El estado

PLAN DE MANEJO						
Plan de acción	**Responsable**	**Fecha de inicio dd/mm/año**	**Fecha de finalización dd/mm/año**	**Fecha de seguimiento dd/mm/año**	**Seguimiento**	**Estado**

TABLA 8 PLAN DE MANEJO DEL RIESGO
Fuente: Adoptado - Adaptada de Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 Versión 6

10.5 Análisis de riesgos de corrupción

Para el establecimiento de los riesgos de corrupción, El Ministerio de Igualdad y Equidad toma como base, la metodología establecida en la Guía para la Administración de Riesgos y establecimientos de controles del DAFP, en relación con los riesgos de corrupción.

El riesgo de corrupción es: "la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado"[8].

En la descripción de los riegos de corrupción concurran cuatro (4) componentes para su definición:

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

Una vez se haya realizado el ejercicio de la identificación de riesgos de corrupción, en el formato OAP-EE-FO-009 Mapa de Riesgos, se registran los riesgos identificados, correspondiente a cada proceso, se clasifican de acuerdo con tipo de riesgo que pertenezca; en este caso fraude interno o fraude externo.

[8] Guía para la administración de riesgos y establecimientos de controles DAFP-2018 V4

10.5.1 Valoración de los riesgos de corrupción

Para la valoración de los riesgos de corrupción, se determina la probabilidad de acuerdo con la metodología establecida para los riesgos de gestión, descrita en el numeral 10.2.2 del presente manual y se clasifican, según la tabla de frecuencia y probabilidad.

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

TABLA 21 CRITERIOS PARA DEFINIR EL NIVEL DE PROBABILIDAD
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Para el cálculo de la probabilidad, se hace necesario resaltar que la frecuencia a la que se hace referencia para los riesgos de corrupción se relaciona con la ejecución de la actividad de la cual proviene el riesgo de corrupción. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo[9].

Determinación del impacto.

Para determinar el impacto de los riesgos de corrupción, se tiene en cuenta los siguientes criterios, de acuerdo con el cuadro CRITERIOS PARA CALIFICAR EL IMPACTO -RIESGOS DE CORRUPCIÓN, el cual permite establecer la zona de impacto de los riesgos de corrupción de acuerdo con las siguientes preguntas:

[9] Guía para la administración de riesgos y establecimientos de controles DAFP-2018 V4

CRITERIOS PARA CALIFICAR EL IMPACTO -RIESGOS DE CORRUPCIÓN		
PREGUNTA: SI EL RIESGO SE MATERIALIZA PODRÍA:	**SI**	**NO**
1 ¿Afectar al grupo de funcionarios del proceso?		
2 ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3 ¿Afectar el cumplimiento de misión de la		
3 ¿Afectar el cumplimiento de misión de la entidad?		
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5 ¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6 ¿Generar pérdida de recursos económicos?		
7 ¿Afectar la generación de los productos o la prestación de servicios?		
8 ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9 ¿Generar pérdida de información de la entidad?		
10 ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11 ¿Dar lugar a procesos sancionatorios?		
12 ¿Dar lugar a procesos disciplinarios?		
13 ¿Dar lugar a procesos fiscales?		
14 ¿Dar lugar a procesos penales?		
15 ¿Generar pérdida de credibilidad del sector?		
16 ¿Ocasionar lesiones físicas o pérdida de vidas humanas		
17¿Afectar la imagen regional?		
18 ¿Afectar la imagen nacional?		
19 ¿Generar daño ambiental?		
SUMA DE X's	0	0

CATASTRÓFICO

TABLA 292 CRITERIOS PARA CALIFICAR EL IMPACTO DE RIESGOS DE CORRUPCIÓN
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

CALIFICACIÓN IMPACTO	
RESPUESTAS POSITIVAS	**IMPACTO**
1 A 5	**MODERADO**
6 A 11	**MAYOR**
12 A 19	**CATASTRÓFICO**
Si la pregunta 16 es afirmativa es Catastrófico	

Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Determinación del riesgo inherente y residual.

Para la determinación del riesgo inherente (antes de controles) y residual, se realiza de acuerdo con lo establecido para los riesgos de gestión, a través de la matriz de calor para establecer la calificación inicial del riesgo. Ver Numerales 10.2, 10.3 Y 10.4, del presente manual.

%	MATRIZ CALIFICACIÓN DE RIESGOS IMPACTO						
100%	Muy alta	ALTA	ALTA	ALTA	ALTA	EXTREMA	
80%	Alta	MODERADA	MODERADA	ALTA	ALTA	EXTREMA	
60%	Media	MODERADA	MODERADA	MODERADO	ALTA	EXTREMA	
40%	Baja	BAJA	MODERADA	MODERADO	ALTA	EXTREMA	
20%	Muy baja	BAJA	BAJA	MODERADO	ALTA	EXTREMA	
	PROBABILIDAD	LEVE	MENOR	MODERADO	MAYOR	CATASTROFICO	
		20%	40%	60%	80%	100%	
		IMPACTO					

Zona de calificación riesgos de

TABLA 23 MATRIZ EVALUACIÓN DE RIESGO DE CORRUPCIÓN
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

10.5.2 Control y seguimiento

El control y el seguimiento para este tipo de riesgos debe ser continua no solo por que cumple una función preventiva sino que también permite la mejora constante de los procesos, la identificación de buenas prácticas y la adaptación oportuna de

controles, permite realizar un ajuste dinámico y una respuesta inmediata a vulnerabilidades detectadas según nuevos patrones de riesgo.

El control y seguimiento será el establecido en el numeral **11.1** del presente documento.

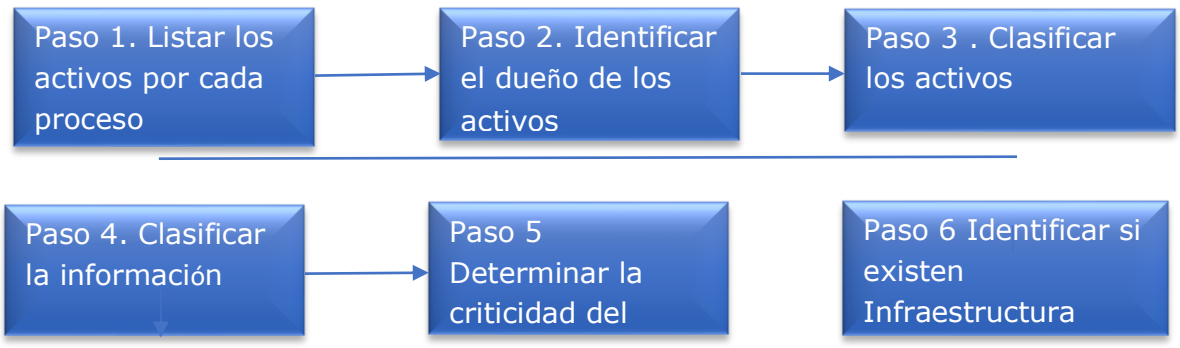
10.6 Análisis de riesgos de Seguridad Digital

El análisis de riesgos de seguridad digital para El Ministerio de Igualdad y Equidad se realiza en base al Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MGRSD, establecido por MINTIC y ANEXO 4: Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas de Función Pública.

10.6.1 Identificación de activos de seguridad digital

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento. Es necesario que la entidad pública identifique los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado. La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública. Para la generación de este inventario, la entidad pública debe tener en cuenta los siguientes pasos:

ESQUEMA 6 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN



Fuente: Pasos para la identificación y valoración de activos. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Identificación de Infraestructuras Críticas Cibernéticas (ICC).

Una vez realizada la identificación, clasificación y valoración de los activos de información, y determinada la importancia de estos para El Ministerio, el proceso encargado del inventario de activos identifica si cuenta con ICC o si alguno de los activos identificados corresponde a una ICC y verifica si su impacto o afectación supera alguno de los criterios siguientes:

Impacto Social: La variable de población se define teniendo en cuenta el establecimiento del contexto externo de la ART, es decir, que la consideración de la población va a estar asociada a las personas a las cuales se les presta servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectados por la materialización de algún riesgo en los activos identificados como ICC.

Impacto Económico: La variable presupuesta es la consideración del presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

Impacto Ambiental: La variable ambiental estará alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Podría no ser utilizada en la mayoría de los casos.

Nota. Si la entidad cuenta con ICC esta es reportada al CCOCI

ID ACTIVO	NOMBRE DEL ACTIVO	NIVEL DE CRITICIDAD ACTIVO	ICC			
			SOCIAL 250.OOO PERSONAS	ECONOMICO	AMBIENTAL	SE DEBE REPORTAR ACCOCI
Indicador ID del activo	Indicador nombre del activo	Indicar Nivel de criticidad, definido en la tabla de registro de activos	Indicar con una X si hay afectación social	Indicar con una X si hay afectación económica	Indicar con una X si hay afectación ambiental	Indicar con una X si se debe reportar a CCOCI

TABLA 24 INDICADORES DE INFRAESTRUCTURA
Fuente: Modelo de gestión de riesgos de seguridad digital MINTIC

10.6.2 Metodología para la identificación de riesgos de SD.

El propósito de la identificación de los riesgos de Seguridad Digital-RSD, es determinar que podría suceder para que cause una perdida potencial, y llegar a comprender el cómo, el dónde, y el por qué podría ocurrir está perdida. Las siguientes etapas del análisis de riesgos de SD se requieren para recolectar datos de entrada para esta actividad.

Para la identificación de los riesgos inherentes El Ministerio de Igualdad y Equidad tiene en cuenta las amenazas y vulnerabilidades asociadas a cada activo de información.

Se identifican tres (3) clases de riesgos inherentes a seguridad digital:

Integridad: se refiere a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros no autorizados.

Confidencialidad: se refiere a cómo los datos se mantienen al acceso únicamente de las personas o sistemas que se encuentran autorizados.

Disponibilidad: se refiere al acceso de la información en el momento que debe estar disponible; se aclara que la información de la entidad no debe estar disponible todo el tiempo durante el año

Para la identificación de los riesgos inherentes, se debe partir de la base que sólo se realizará análisis de los potenciales riesgos en seguridad digital a los activos considerados como críticos en una primera Fase, con el fin de priorizar la gestión de riesgos y controles de seguridad digital. Para esta identificación, El Ministerio de Igualdad y Equidad tiene en cuenta las amenazas y vulnerabilidades asociadas a cada activo de información.

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

"La gestión de riesgos en seguridad de la información que cubre la identificación, valoración y evaluación de riesgos se realiza tomando como insumo la identificación de los activos de información, posterior a ello, se realizan mesas de trabajo con el responsable de seguridad de información y cada uno de los líderes de proceso (o a quien este designe). La valoración de los riesgos se hace a través

de juicios de experto y cuando aplique, basado en datos previos con los que cuente la Entidad. Finalmente, una vez identificado los riesgos de seguridad, y de acuerdo con los niveles de valoración y aceptación, se define en conjunto con el líder de proceso la propuesta de plan de tratamiento de riesgos para ser revisado, aprobado, implementado y monitoreado por las partes."

NOTA: *Para efectos de gestión de riesgos se considerarán aspectos de la metodología de gestión de riesgos establecida por el Departamento de la Función Pública, de la cual se extraerán elementos que se consideren pertinentes, sin obligatorio cumplimiento en su totalidad.*

En el siguiente numeral, se detallan algunas amenazas que pueden hacer daños a los activos y materializar los riesgos y algunas vulnerabilidades (debilidades) descritas en el *anexo 4. Lineamientos para la GRSD y complementadas por la Guía De Gestión De Riesgos emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Digital para la Seguridad y privacidad de la información.*

De acuerdo con lo descrito en la *Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas" del DAFP,* para la identificación del riesgo y el análisis de las posibles amenazas y vulnerabilidades que podrían causar la materialización de este, El Ministerio de Igualdad y Equidad ha adoptado la siguiente tabla:

Riesgo	Descripción del riesgo	Activo	Tipo de Activo	Amenaza	Vulnerabilidades	Consecuencia/Impacto
Identificar el tipo de riesgo de acuerdo con la identificación establecida	Detallar el riesgo	Asociar activo o grupo de activos según lo identificado en el formato de registro de activos de información	Detallar el tipo de activo de información	Detallar la amenaza a la cual está expuesta el grupo de activo	Describir cuales son las vulnerabilidades asociadas a la amenaza identificada.	Describir las consecuencias que tendría el grupo de activos al verse afectado por la amenaza asociada.

TABLA 25 GUÍA PARA LA IDENTIFICACIÓN DEL RIESGO
Fuente: DAFP v6

Una vez se haya realizado el ejercicio de la identificación de activos, se continúa con la identificación de los RSD, en el formato Matriz Riesgos de SD y Anexos, en la cual se registran los riesgos de SD y la información que se establece en la Matriz, para tal fin.

10.6.3 Establecimiento de controles de riesgos de Seguridad Digital

Para establecer los controles para los riesgos de Seguridad Digital se debe tener en cuenta:

- La selección de los controles implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales, por lo tanto, se deberá considerar aspectos como:
- Viabilidad jurídica: Velar por que los controles que se van a implantar no vayan en contra de la normatividad vigente.
- Viabilidad técnica e institucional: Establecer claramente si el Ministerio está en capacidad de implantar y sostener a largo plazo nuevas tecnologías u otros mecanismos necesarios para ejecutar el control.
- Análisis de costo-beneficio: Prácticamente todas las respuestas a los riesgos implican algún tipo de costo directo o indirecto que se debe sopesar en relación con el beneficio que genera. Se ha de considerar el costo inicial del diseño e implementación de una respuesta (procesos, personal, tecnología), así como el costo de mantener la respuesta de forma continua.

- Este caso se puede dar específicamente para aquellos controles nuevos que requieren contrataciones adicionales a los funcionarios que desarrollan los proceso o bien cuando se requiere diseñar e implementar sistemas de información o tecnologías específicas para ejecutar el control.

El Modelo de Seguridad y Privacidad de la Información del Ministerio de Igualdad y Equidad en su fase de Planificación deberá realizar la selección de controles de seguridad digital que correspondan para el tratamiento del riesgo, y durante la fase Implementación deberá ejecutar la implementación de dichos controles, por lo cual se cuenta con el anexo de controles del estándar ISO 27001.

NOTA: *El Ministerio deberá determinar si ya posee alguno de estos controles del Anexo A de la Norma ISO 27001 2022 o si deberá aplicar alguno para realizar luego el tratamiento del riesgo residual.*

A partir de esta metodología se establece una matriz de riesgos de seguridad digital que contempla la asignación de valores y atributos a la probabilidad de ocurrencia de una amenaza afectando la seguridad de los activos de información, al igual que los valores y atributos sobre el impacto que afectan al Ministerio producto de la materialización de los riesgos. Adicionalmente, en la matriz de riesgos**,** se encuentran identificados los controles existentes y la evaluación del riesgo residual que necesariamente debe ser gestionada a través de implementación de controles propuestos en el tratamiento de los riesgos, lo cual obedece a la metodología para la valoración de los controles, acorde con la de los riesgos de gestión.

Identificación y evaluación de controles Seguridad Digital:

Para los casos en los cuales se determine Reducir el Riesgo o Compartir el riesgo se deben estructurar controles que cumplan con las características establecidas en el presente documento.

Tipo de controles.

Los tipos de controles son los mismos que se han establecido para los riesgos de gestión corrupción, estos son:

Controles Preventivos: Son los que actúan en la entrada del proceso y antes de que se realice la actividad que origina el riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Controles detectivos: Son los que actúan durante la ejecución de la actividad. Detectan el riesgo, pero generan reprocesos.

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

De acuerdo con la forma como se ejecutan los controles, se clasifican en:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Se propenderá estructurar un Control que permita dar cobertura de carácter preventivo, detectivo y correctivo, los cuales deben tener las características de un control.

Los controles de Seguridad Digital tienen las mismas características de los riesgos de gestión y corrupción, conforme a la metodología establecida en el Numeral **10.3.1 Estructura de los Controles,** del presente documento.

10.7 Análisis de Riesgo Fiscal

Para el establecimiento de los riesgos de corte fiscal, El ministerio toma como base, la metodología establecida en la Guía para la Administración de Riesgos y establecimientos de controles del DAFP,

El riesgo fiscal es: "Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial"[10].

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

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: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, 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. En esta guía, el evento potencial es equivalente a la causa raíz.

Lo anterior se puede resumir de la siguiente manera:

***Riesgo Fiscal* =** Evento Potencial (Potencial Conducta) **+** Efecto dañoso

[10] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

Una vez se haya realizado el ejercicio de la identificación de riesgos de corrupción, en el formato OPA-EE-FO-008 Mapa de Riesgos, se registran los riesgos identificados, correspondiente a cada proceso, se clasifican de acuerdo con tipo de riesgo que pertenezca; en este caso **bienes públicos, recursos públicos o intereses patrimoniales de naturaleza pública.**

10.7.1 Identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer 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 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[11].

Para las circunstancias inmediatas, se trata de aquella situación o actividad 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.

10.7.1.1 Descripción del Riesgo Fiscal

Para redactar un riesgo fiscal se debe tener en cuenta:

Iniciar con la oración: *Posibilidad de,* debido a que nos estamos refiriendo al evento potencial.

Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

[11] Articulo 3 ley 610 de 2000

Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera[12].

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato

TABLA 106 EJEMPLO DE BIENES
Fuente: Guía para la Administración de Riesgos y establecimiento de controles DAFP-2022 V.6

Valoración del Riesgo Fiscal

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

Determinación de la probabilidad.

Para la valoración de los riesgos fiscales, se determina la probabilidad de acuerdo con la metodología establecida para los riesgos de gestión, descrita en el numeral **10.2.2** del presente documento y se clasifican, según la tabla de frecuencia y probabilidad.

[12] El control y la responsabilidad fiscal en Colombia. Luz Jimena Duque Botero y Freddy Céspedes Villa Ibáñez. 2018.

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

TABLA 11 CRITERIOS PARA DEFINIR EL NIVEL DE PROBABILIDAD
Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Determinación del impacto.

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.

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

IMPACTO			
Nivel	**% Impacto**	**Afectación Económica**	**Reputacional**
Catastrófico	**100%**	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

TABLA 128 CRITERIOS PARA DEFINIR EL NIVEL DE IMPACTO
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

Determinación del riesgo inherente y residual.

Para la determinación del riesgo inherente (antes de controles) y residual, se realiza de acuerdo con lo establecido para los riesgos de gestión, a través de la matriz de calor para establecer la calificación inicial del riesgo. Ver Numerales 8.2, 8.3 y 8.4, del presente documento.

	%		IMPACTO				
PROBABILIDAD	100%	Muy alta					
	80%	Alta					
	60%	Media					
	40%	Baja					
	20%	Muy baja					
			LEVE 20%	MENOR 40%	MODERADO 60%	MAYOR 80%	CATASTROFICO 100%
			IMPACTO				

TABLA 13 EVALUACIÓN DE LOS RIESGOS
Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2022 V.6

10.8 Mapas de Riesgos

El mapa de riesgo es el consolidado de los riesgos identificados en cada proceso, los riesgos residuales, planes de manejo y planes de contingencia. El mapa de cada proceso cuenta con el Formato OAP-EE-FO-009 Mapa de Riesgos y del formato OAP-EE-FO-008**.**

Los mapas de riesgos permiten llevar el control de los riesgos, a nivel de proceso y a nivel estratégico.

Los Mapas de Riesgo son consolidados por la Oficina de Planeación y se clasifican en:

Mapa de Riesgo de Proceso: El cual contiene los riesgos identificados en cada uno de los procesos. Estos mapas deben ser revisados por el director, subdirector, jefe de Oficina, Coordinador de Grupo o Líder de Proceso; y deben ser aprobados por el Líder del Proceso.

Mapa de Riesgo de Institucional: El cual consolida los riesgos identificados en cada proceso calificados en zona alta y extrema y los riesgos de corrupción. Este es consolidado por la Oficina de Planeación.

11. MONITOREO Y SEGUIMIENTO

11.1 Monitoreo de los riesgos y controles.

El monitoreo a los mapas de riesgos es esencial para asegurar la eficiencia y eficacia de las acciones establecidas para el tratamiento de los riesgos de gestión, seguridad digital, fiscal y de corrupción, la cual se adelanta a través del monitoreo, seguimiento y revisión periódica, de tal forma que permita evidenciar todas aquellas situaciones o factores que puedan influir en el resultado de las acciones

11.1.1 procedimiento para la ejecución de controles:

El primer paso fundamental consiste en desarrollar un inventario exhaustivo y sistemático de todos los controles existentes en el mapa de riesgos, lo cual implica identificar y documentar detalladamente cada control activo, incluyendo su propósito, responsable, frecuencia de ejecución y el riesgo específico que busca mitigar. Este proceso debe comenzar con una recopilación de información a través de reuniones con los dueños de procesos, revisión de documentación existente y validación de procedimientos actuales, asegurándose de registrar cada control en una matriz estructurada que incluya elementos como el código identificador único, nombre descriptivo, tipo de control (preventivo, detectivo o correctivo), estado actual, última fecha de revisión, responsables tanto de ejecución como de supervisión, proceso al que pertenece. Es crucial que esta actividad inicial se realice de manera metódica y detallada, ya que servirá como base fundamental para todas las actividades subsecuentes del proceso de gestión y control de riesgos, permitiendo establecer un punto de referencia claro para el seguimiento

y la evaluación futura de la efectividad de los controles, es necesario realizar una evaluación detallada de la efectividad y funcionamiento de cada control identificado realizando:

ESQUEMA 7 EJECUCIÓN DE CONTROLES

Fuente: Ministerio De Igualdad y Equidad

Luego de completar el análisis de los controles existentes, el siguiente paso consiste en desarrollar e implementar un plan de acción integral que aborde todas las deficiencias y oportunidades de mejora identificadas. Este plan debe incluir acciones correctivas específicas con responsables claramente designados, plazos de implementación realistas, recursos necesarios y métricas de seguimiento definidas. Es fundamental proceder con el rediseño de controles inefectivos, la creación de nuevos controles donde se identificaron brechas, la actualización de procedimientos y documentación relacionada, así como la implementación de mejoras cuando sea necesario. Todo esto debe ir acompañado de un proceso robusto de comunicación y capacitación para el personal involucrado, seguido por un de monitoreo continuo que incluya revisiones periódicas, evaluaciones de efectividad y actualizaciones de las matrices de riesgo y control. Esta fase es crucial para asegurar que las mejoras implementadas realmente fortalezcan el sistema de control de riesgos de la organización.

El monitoreo a los mapas de riesgos, *la realizará los Líderes de Proceso*, con el apoyo de los gestores, de acuerdo con la periodicidad establecida en la Política de Administración de Riesgos y las responsabilidades establecidas.

Para la ejecución de todos los controles establecidos en la matriz de riesgos institucional, es obligatorio el diligenciamiento del Formato OAP-EE-FO-013 Control y seguimiento de riesgos, el cual constituye la evidencia formal del seguimiento y efectividad de los controles implementados.

11.2 lineamientos para la modificación de controles ante cambios en procesos:

En el marco del seguimiento y monitoreo continuo al Sistema de Gestión de Riesgos, cuando se identifica una modificación o cambio en alguno de los procesos institucionales que pueda afectar la efectividad de los controles establecidos (sean estos riesgos de gestión, corrupción, seguridad digital, o de cualquier otra naturaleza), es fundamental implementar un procedimiento sistemático y documentado que permita actualizar, fortalecer y adaptar las medidas de control existentes. Este procedimiento busca garantizar que los cambios en los procesos no generen vulnerabilidades, Incrementan la probabilidad de materialización de riesgos, asegurando así la continuidad y efectividad de las operaciones institucionales. A continuación, se detallan los pasos a seguir cuando se detecta una modificación en los procesos que requieren ajustes en los controles de riesgos:

- **RESPONSABLES**

- Líderes de proceso
- Oficina de Planeación
- Comité Institucional de Coordinación de Control Interno
- Oficina de Control Interno
- Gestores de Riesgo designados

- **PROCEDIMIENTO**

Identificación del Cambio

Responsable: Líder del Proceso

- Documentar la modificación identificada en el proceso
- Evaluar el impacto preliminar sobre los controles existentes
- Notificar a la Oficina de Planeación sobre los cambios detectados
- Registrar en el formato Solicitud de Modificación de Controles

- **Análisis del Impacto**

Responsable: Oficina Asesora de Planeación y Líder del proceso

- Realizar mesa de trabajo para evaluar el impacto del cambio.
- Identificar controles afectados
- Evaluar la efectividad actual de los controles
- Determinar la necesidad de nuevos controles.
- Diseñar nuevos controles si se requieren
- Definir recursos necesarios
- Establecer cronograma de implementación

- **Aprobación**
- **Responsable :** Comité Institucional de Coordinación de Control Interno

Presentar propuesta de modificación
Evaluar viabilidad de cambios
Aprobar o solicitar ajustes

- **Implementación**

Responsable : Líder del Proceso

- Socializar cambios aprobados
- Actualizar documentación del proceso
- Capacitar al personal involucrado
- Implementar nuevos controles
- Registrador de evidencias de implementación

- **Seguimiento**

Responsable: Oficina de Control Interno

- Verificar implementación de cambios
- Evaluar efectividad de nuevos controles
- Generar informe de seguimiento
- Proponer ajustes si se requieren

12. PRESENTACIÓN DEL INFORME DE GESTIÓN DE RIESGOS POR LA SEGUNDA LÍNEA DE DEFENSA

la Oficina Asesora de Planeación, como segunda línea de defensa del Sistema, tiene la responsabilidad de consolidar y presentar el informe de gestión de riesgos ante la Alta Dirección, con el propósito de facilitar la toma de decisiones estratégicas basadas en una evaluación integral del Sistema. De la Gestión de Riesgos institucionales. A continuación, se detallan las responsabilidades y características fundamentales de este proceso:

- Recopila información de la primera línea (líderes de proceso)
- Incorporar resultados del monitoreo periódico.
- Valida datos con las áreas responsables
- Analiza tendencias y patrones
- Recomendaciones
- Primera Línea: Proporciona información sobre la ejecución de controles
- Tercera Línea (Control Interno): Informe de resultados de evaluaciones independientes

Contenido del informe:

- Estado general de la gestión de riesgos
- Nivel de cumplimiento de controles
- Riesgos materializados
- Efectividad de los controles
- Recomendaciones de mejora
- Recopilación de lesiones aprendidas

Este informe constituye una herramienta fundamental para la toma de decisiones estratégicas y el fortalecimiento continuo del Sistema de Gestión de Riesgos institucional.

12.1 Seguimiento a los mapas de riesgos.

La Oficina de Planeación, será quien apoye a la entidad, en el seguimiento periódico a los Planes de Manejo establecidos en los Mapas de Riesgos de gestión, fiscal y de corrupción y los Planes de Manejo de los riesgos de Seguridad Digital se hará

acorde con las roles y responsabilidades dadas al responsable de seguridad de la información del Ministerio.

El Grupo Interno de Trabajo de Control Interno del Ministerio o quien hace sus veces, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación o quien haga sus veces. (Guía Administración Riesgos V.6 DAFP)

12.2 Seguimiento Riesgos de Corrupción.

Para el caso de los riesgos de corrupción, el seguimiento y publicación, se realizará de acuerdo con lo establecido en el Programa de Transparencia y Ética Publica V1 y la metodología establecida en la Guía para la Administración de Riesgos y Diseño de Controles en entidades públicas del DAFP.

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

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en
- la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Generalidades:

13. LINEAMIENTOS PARA LA SEGREGACIÓN DE FUNCIONES EN PROCESOS CRÍTICOS

La segregación de funciones constituye un control transversal determinante en el Sistema de Gestión de Riesgos del Ministerio de Igualdad y Equidad, actuando como barrera preventiva frente a posibles eventos de riesgo operativo, fraude o corrupción. Este principio, fundamentado en la Ley 87 de 1993 y alineado con la Guía de Administración del Riesgo del DAFP, representa una clave de control para

mitigar los riesgos inherentes en procesos críticos, especialmente aquellos relacionados con el manejo de recursos públicos, toma de decisiones y custodia de bienes. La adecuada segregación de funciones reduce la probabilidad de materialización de riesgos al evitar la concentración de funciones incompatibles en un mismo servidor público, fortaleciendo así las tres líneas de defensa del Sistema de Control Interno. El Ministerio, en su compromiso con una gestión efectiva del riesgo, establece los siguientes lineamientos normativos y recomendaciones prácticas para implementar y mantener una segregación de funciones que contribuya eficazmente al tratamiento de riesgos institucionales:

13.1 Reporte resultado del monitoreo y seguimiento

La identificación y valoración de factores que pueden generar nuevos riesgos en la entidad requiere un análisis sistemático y continuo del contexto organizacional. Este proceso debe considerar la naturaleza dinámica tanto del entorno como de la institución, evaluando el impacto potencial de los cambios sobre los objetivos estratégicos y operativos. Para una evaluación efectiva, es fundamental realizar un monitoreo constante de las variables externas que pueden afectar la gestión institucional, tales como: modificaciones en políticas públicas, cambios normativos, variaciones presupuestales, transformaciones sociales, avances tecnológicos y nuevas demandas de la ciudadanía. Simultáneamente, se debe mantener una vigilancia activa sobre los factores internos como: cambios en la estructura organizacional, rotación de clave personal, modificaciones en procesos y procedimientos, actualizaciones tecnológicas, y variaciones en la capacidad operativa. Esta evaluación debe realizarse mediante métodos estructurados que incluyan la participación de las diferentes áreas y niveles de la organización, documentando sistemáticamente los hallazgos y estableciendo mecanismos de seguimiento que permitan identificar oportunamente la necesidad de ajustar controles o implementar nuevas medidas de tratamiento como revisar informes y análisis de casos y experiencias previas, monitoreo de indicadores clave, áreas o procesos afectados.

Se deben establecer mecanismos de actualización: como Revisiones programadas, evaluaciones extraordinarias, seguimiento continuo, participación multidisciplinaria.

Cuando se determine que se los mapas de riesgo deben ser modificados, como resultado de este análisis o del resultado del seguimiento que realice el Grupo Interno de Trabajo de Control Interno, o los diferentes entes de control, se debe:

Reportar a la Oficina de Planeación, con el fin de actualizar los mapas correspondientes, en cualquiera de sus componentes, ya sea a los riesgos, sus causas, consecuencias, controles, tratamientos o planes de manejo.

Si se identifican cambios internos o externos que puedan impactar positiva o negativamente a la Entidad o algún proceso, se reporta a la Oficina de Planeación, con el fin de apoyar la identificación, análisis y valoración de riesgos de gestión o corrupción del proceso. seguir procedimiento numeral 11.2 del presente documento.

Los reportes que se hagan a la Oficina de Planeación se deben realizar a través de correo electrónico, soportado con la Matriz de Riesgos de Gestión y cuando se trata de los riesgos de SD, se debe comunicar a la Oficina de Tecnologías de la Información, con copia al responsable de seguridad digital.

Cuando se realice el *monitoreo de los riesgos de corrupción*, se debe reportar el resultado de este al GIT de Control Interno según las fechas que éste determine y de acuerdo con los cortes cuatrimestrales establecidos en el numeral 11.2 del presente documento y a la Oficina de Planeación.

La Oficina de Planeación, será la encargada de consolidar el Mapa de Riesgos Institucional y presentar al Comité de Institucional de Gestión y Desempeño y/o al Comité Institucional de Coordinación de Control Interno el resultado del monitoreo y seguimiento que se realice a los mismos, con el fin de establecer la necesidad de definir si es necesario la revisión y ajuste de la Política de Riesgos del Ministerio o se deba tomar acciones sobre riesgos estratégicos, o de corrupción que presenten una alta probabilidad de materializarse.

14. SOCIALIZACIÓN Y COMUNICACIÓN

La comunicación y divulgación de la política y la metodología para la administración de los riesgos, será dada a conocer por la Oficina de Planeación, en coordinación con la Oficina de Comunicaciones, la cual se realizará a través de los diferentes

medios de comunicación interna, con el fin de dar cubrimiento al mayor número de servidores públicos de la Entidad, tanto a nivel central, como a nivel territorial.

Así mismo, los líderes de proceso con el apoyo de los gestores socializarán la política y los mapas de riesgos a los equipos de trabajo, así como los cambios y actualizaciones que se llegarán a generar, dejando registro de estas.

15. Fechas de seguimientos y publicación.

El seguimiento se realiza tres (3) veces al año, así:

Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.

Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10), primeros días hábiles del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero"[13]**.**

Para el seguimiento de los riesgos de corrupción, se podrá utilizar el formato del Anexo 6 Matriz de seguimiento a los riesgos de corrupción de la Guía del DAFP.

16. CONTROL DE CAMBIOS

Cuando se requiera modificar o actualizar la Política de Administración de Riesgos, en relación con la política, la metodología para la gestión de riesgos, lo realizará la Oficina de Planeación y se presentará en el Comité Institucional de Coordinación Control Interno, para ser aprobado por parte del Representante Legal Ministerio de conformidad con el literal g del artículo 2.2.21.1.6 del Decreto 1083 de 2015. (Funciones del Comité)

[13] Guía para la administración de riesgos y establecimientos de controles DAFP-2022 V6

"*Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta"*

La actualización, modificación, ajuste y publicación de la Política estará a cargo de la Oficina de Planeación y se publicará con las versiones actualizadas en el repositorio y en la página web de la Entidad en el enlace de transparencia. Las modificaciones o actualización de versiones a la política, sus anexos y formatos para la gestión de riesgos, que no impliquen cambios en la política y metodología serán realizadas por la Oficina de Planeación, cuando así se requiera y publicadas con las versiones actualizadas, en el repositorio y en la página web de la Entidad en el enlace de transparencia