POLITICA PARA LA ADMINISTRACIÓN DEL RIESGO 2023

INSTITUTO DE MOVILIDAD DE PEREIRA
NIT 816.000.558-8
GESTIÓN GERENCIAL

PEREIRA, RISARALDA
2023

Este documento presenta la policita de administración del Riesgo del Instituto de Movilidad de Pereira con actualización a la vigencia 2023, esta cuenta con el siguiente contenido:

Contenido

1. INTRODUCCION

El Departamento Administrativo de la Función Pública, mediante el Decreto 1499 de 2017, determinó que las entidades públicas debían implementar el Modelo Integrado de Planeación y Gestión - MIPG, que integra los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998); que crea un único Sistema de Gestión, articulado con el Sistema de Control Interno (Ley 87 de 1993), el cual se actualiza a través de Modelo Estándar de Control Interno - MECI y el Esquema de Líneas de Defensa Lo anterior, con el fin de entregar a los ciudadanos lo mejor de la gestión y en consecuencia, producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción.

El Instituto De Movilidad De Pereira (IMP), como entidad pública, está al servicio de la comunidad. Por lo tanto, obligación de sus servidores públicos y contratistas, actuar con honestidad, respeto, compromiso, diligencia y justicia, para proteger y hacer correcto uso de los activos y recursos que han sido asignados para nuestra debida administración. Es así como se deben tomar todas las medidas necesarias con el objeto de evitar o mitigar cualquier riesgo que se presente en la entidad.

Para ello, se establece que todas las entidades públicas deben contar con una política que facilite la administración de los riesgos, a fin de alcanzar sus objetivos institucionales de manera más eficiente, adelantándose a aquellos eventos que puedan poner en peligro su gestión, por medio del autocontrol y la autoevaluación.

Teniendo en cuenta que la administración de riesgos es estratégica para el logro de los objetivos institucionales y de procesos, en este documento se enuncia la política que permitirá tomar decisiones relativas a la administración de los diferentes riesgos (Gestión, Corrupción, Fiscal y Seguridad Digital), inmersos en el desarrollo de la gestión, lo cual está alineado y armonizado con el Modelo Integrado de Planeación y Gestión (MIPG), la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, definida por el Departamento Administrativo de la Función Pública (DAFP), articulada con la normativa aplicable a la Entidad.

A través de esta Política, se establecen los principios necesarios para hacer que la administración y gestión del riesgo sea eficaz, eficiente y coherente, siendo necesario que se implemente en todos los niveles del Instituto de Movilidad De Pereira (IMP)– Nivel Central, así como en los proyectos y actividades que desarrolla, teniendo en cuenta su contexto, las partes involucradas y la diversidad de criterios de riesgos, entendiendo el riesgo como una oportunidad de mejora, que bien aprovechada sirve

como herramienta para optimizar los resultados, a corto, mediano y largo plazo. En este documento, que contiene la declaración e intención de la Alta Dirección, con respecto a la gestión del riesgo, se establecen los lineamientos precisos acerca del tratamiento, manejo y seguimiento de estos.

2. OBJETIVOS

2.2 Objetivo General

Establecer los lineamientos y criterios, que permitan la correcta identificación, análisis, valoración y Administración de los riesgos de gestión, corrupción y seguridad digital; minimizando el impacto que estos puedan tener en el logro de los objetivos institucionales y de todos los procesos del IMP.

2.3 Objetivo Específicos

- Identificar los riegos inherentes a todos los procesos del IMP; con el fin de realizar las acciones necesarias para la reducción, prevención, mitigación y atención de efectos negativos de una posible ocurrencia de alguno de estos.
- Documentar los controles aplicables a cada riesgo de acuerdo con el proceso que pertenecen.
- Aplicar los controles tendientes a la prevención de la materialización de los riesgos identificados por cada Subproceso del IMP.
- Establecer un mecanismo y periodicidad para la difusión y apropiación de la política de riesgos por parte de toda la entidad.
- Desarrollar estrategias que conlleven a un efectivo seguimiento, monitoreo, y mitigación de los riesgos.
- Definir la administración del riesgo como una herramienta que permita realizar una mejora continua de todos procesos internos y externos del IMP.

3. ALCANCE

La Política Institucional de Administración del Riesgo es aplicable a todas las áreas del modelo de operación por procesos, a los planes institucionales, a los programas, a los proyectos y a las acciones ejecutadas por los servidores públicos y contratistas de

prestación de servicios del IMP; así como a los lineamientos para el tratamiento, manejo y seguimiento a los riesgos de gestión, corrupción, y seguridad digital.

4. TERMINOS Y DEFINICIONES

Las siguientes definiciones fueron tomadas de la guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública en su versión 6, de noviembre del 2022:

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

Actitud hacia el riesgo: Enfoque del Instituto de Movilidad Pereira con respecto a los riesgos, esto incluye una evaluación que implica decisiones como retener, tomar o alejarse del riesgo.

Análisis del riesgo: Es el conjunto de acciones, recursos y métodos para comprender la naturaleza del riesgo. Este proceso soporta la evaluación del riesgo y las decisiones relacionadas con el tratamiento del riesgo.

Apetito de Riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Áreas de impacto: Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un 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.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata).

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Causa Raíz (Causa Eficiente o Causa Adecuada): Es el evento (acción u omisión) que de

presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

Confidencialidad: Propiedad de la información que la hace no disponible o sea 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.
Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.

Control: Medida que permite reducir o mitigar un riesgo.

Consecuencia: Es el resultado de un evento que afecta los objetivos de la entidad, esta consecuencia puede ser expresada de manera cualitativa o cuantitativamente.

Contexto externo: Son las condiciones, tendencias o circunstancias externas con las cuales se busca alcanzar el logro de los objetivos, estas condiciones son de tipo cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo del instituto Movilidad Pereira. Estas condiciones pueden ser de orden nacional o internacional.

Contexto interno: Son condiciones de tipo interno con los cuales se consiguen losobjetivos institucionales y estructurales, éstos últimos van desde la línea de organización jerárquica, la distribución y responsabilidad funcional, la capacidad operativa, entendida como el talento humano, los recursos tecnológicos y económicos, los métodos de trabajo.

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

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

Establecimiento del contexto: Es el conjunto de parámetros internos y externos que se deben tener en cuenta en la gestión del riesgo. Este contexto es el punto de partida parala evaluación y el establecimiento de políticas de gestión del riesgo.

Evaluación del riesgo: Es el proceso utilizado para determinar las prioridades del sistema de administración del riesgo y la decisión de tratamiento acerca del riesgo, esto comparando el nivel de un determinado riesgo con respecto a los criterios del riesgo, determinando de esta forma, si el riesgo, la magnitud de este o ambos se puedenconsiderarse aceptables o tolerables.

Evento: Incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado. Un evento puede ser una o más ocurrencias y ser atribuido a una o más causas.

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

Fuente del riesgo: Es un elemento tangible o intangible que por sí mismo o en combinación tiene el potencial intrínseco de originar un riesgo

Gestión del Riesgo: Se refiere a la arquitectura, entendida esta como los principios y metodología para la gestión eficaz del riesgo, es decir, son un conjunto de actividades coordinadas para dirigir y controlar el IMP con respecto al riesgo.

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)4” . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

Gestor público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales”3. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Impacto: se entiende como las consecuencias que pueden ocasionar a la organización, la materialización del riesgo.

Identificación del riesgo: Es la parte de la valoración del riesgo que encuentra, reconocey describe el riesgo. Es un mecanismo de control, que permite conocer los eventos potenciales

que ponen en riesgo el logro de la misión. El alcance incluye la identificación de las fuentes del riesgo, los eventos, las causas y consecuencias.

Integridad: Propiedad de exactitud y completitud.

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.

Política para la gestión del riesgo: Es la declaración y lineamientos generales de la Alta Dirección con respecto a la gestión del riesgo.

Proceso para la gestión del riesgo: Se entiende como la aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de gestión del riesgo.

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

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

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos

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

Riesgo 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 potencial2.
(ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

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

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

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

Tratamiento del riesgo: Es el proceso para modificar el riesgo. Las decisiones sobre esta modificación implican evitar o tomar el riesgo, retirar la fuente del riesgo, cambiar la probabilidad de ocurrencia del riesgo, cambiar las consecuencias del riesgo, compartir o transferir el riesgo con uno o varios de los actores que tienen incidencia o se afectan con el riesgo y retener el riesgo a través de una decisión informada.

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

Valoración del riesgo: Se define como el producto de verificar los resultados de la evaluación del riesgo con los controles identificados, estableciendo prioridades para su manejo y para la fijación de políticas. Comprende el proceso total de identificación,análisis y evaluación del riesgo.

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

5. NIVELES DE RESPONSABILIDAD SOBRE LA GESTIÓN DEL RIESGOS

La definición de la Política de Administración del Riesgo está a cargo del **Representante Legal de la Entidad**, el **Comité Institucional de Coordinación de Control Interno** y **Comité Institucional de Gestión y Desempeño;** a fin de garantizar una adecuada gestión del riesgo, se requiere el compromiso de todo el personal para cumplir con cada una de las instancias que participan en la definición y ejecución de las acciones, métodos, y procedimientos de control de riesgos.

Cabe resaltar que la primera línea (los líderes de proceso o a quienes corresponde), deben:

1. Identificar y valorar los riesgos que puedan afectar el logro de los Objetivos Institucionales.
2. Definir y diseñar los controles a los riesgos.
3. Cumplir con los planes de acción establecidos para cada uno de los riesgos materializados, establecidos en el Plan de Tratamiento de Riesgos.

A continuación, se detalla cada nivel de responsabilidad frente al riesgo desde las líneas de defensa:

5.1. LINEAS ESTRATEGICAS

RESPONSABLES: Representante Legal de la Entidad, Comité Institucional de Coordinación de Control Interno, Comité Institucional de Gestión y Desempeño.

OBJETIVO: Definen el marco general para la gestión y control del riesgo y supervisan su cumplimiento

RESPONSABILIDAD FRENTE AL RIESGO:

- Revisar los cambios en el Direccionamiento Estratégico y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados.

- Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las Etapas de la Gestión del Riesgos y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.

- Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo con las políticas de tolerancia establecidas y aprobadas.

- Revisar los informes presentados, por lo menos cada trimestre, de los eventos de

riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción; así como las causas que dieron origen a esos eventos de riesgos materializados y aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas; lo anterior mediante el análisis de indicadores asociados a dichos objetivos.

5.1.1. PRIMERA LINEA

RESPONSABLES: Gerentes Públicos, Líderes de proceso.

OBJETIVO: Gestionar los riesgos que puedan afectar el cumplimiento de los objetivos Institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos.

RESPONSABILIDAD FRENTE AL RIESGO:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.

- Verificar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.

- Examinar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.

- Chequear 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.

- Verificar y reportar a planeación, los eventos de riesgos que se han materializado en su proceso, incluyendo los riesgos de corrupción; así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.

- Examinar 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 de los objetivos.

- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la Línea Estratégica, Segunda y Tercer Línea de Defensa con relación a la Gestión de Riesgos.

5.1.2. SEGUNDA LINEA

RESPONSABLES: Subdirector de Planeación, Supervisores e interventores de contratos o proyectos, Líderes de los Sistemas de Gestión.

OBJETIVO: Brindar Asistencia y guía a la Línea estratégica y a la Primera Línea de Defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción; a través del establecimiento de directrices y apoyo en el proceso de identificación, análisis, evaluación y tratamiento de los riesgos, al realizar un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

RESPONSABILIDAD FRENTE AL RIESGO:

- 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 los procesos, con el fin de solicitar y apoyaren la actualización de las matrices de riesgos.

- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.

- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.

- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

5.1.3. TERCERA LINEA

RESPONSABLES: Oficina de Control Interno o Auditoría Interna.

OBJETIVO: Proveer aseguramiento independiente y objetivo sobre la efectividad del Sistema de Gestión de Riesgos, validando que la Línea Estratégica, la 1ra Línea y 2da Línea de defensa cumplan con sus responsabilidades en la Gestión de Riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.

RESPONSABILIDAD FRENTE AL RIESGO:

- 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 los procesos, con el fin de que seidentifiquen y actualicen las matrices de riesgos por parte de los responsables.

- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimientode los objetivos de los procesos, incluyendo los riesgos de corrupción.

- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.

- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de lasauditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.

Además de las líneas de defensa y las responsabilidades designadas en la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas” del DAFP**: V6 de noviembre de 2022”** es necesario indicar las responsabilidades designadas al responsable de Seguridad Digital, de acuerdo con el Modelo Nacional de gestión de riesgos de seguridad

de la información para entidades públicas, establecido por el MinTIC.

6. NIVEL DE RESPONSABILIDAD FRENTE AL RIESGO DE SEGURIDAD DIGITAL.

RESPONSABLE: Subdirector de Sistemas y Telemática del IMP.

RESPONSABILIDAD FRENTE AL RIESGO: 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.

7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

7.1. METODOLOGIA PARA LA IDENTIFICACION, VALORACION Y CONTROL DE LOS RIESGOS

Está fundamentada en la guía para la administración del riesgo y diseño de controles en entidades Públicas (V6 de noviembre de 2022) del Departamento Administrativo de la Función Pública, bajo este entendido, la metodología de administración de riesgos se lleva a cabo a través del desarrollo de las siguientes actividades:

a. Política de Administración del Riesgo
- Lineamientos de la política
- Marco conceptual para el apetito del riesgo

b. Identificación del riesgo
- Análisis de objetivos estratégicos y de los procesos
- Identificación de los puntos de riesgo
- Identificación de áreas de impacto
- Identificación de áreas de factores de riesgo
- Descripción del riesgo
- Clasificación del riesgo

c. Valoración del riesgo
- Análisis de riesgos
- Evaluación del riesgo
- Estrategias para combatir el riesgo
- Herramientas para la gestión del riesgo
- Monitoreo y Revisión

Para lo cual, se adopta el formato de Excel Matriz de Riesgos para facilitar el proceso de identificación, valoración y tratamiento de los riesgos.

7.1.1. IDENTIFICACION DE RIESGOS

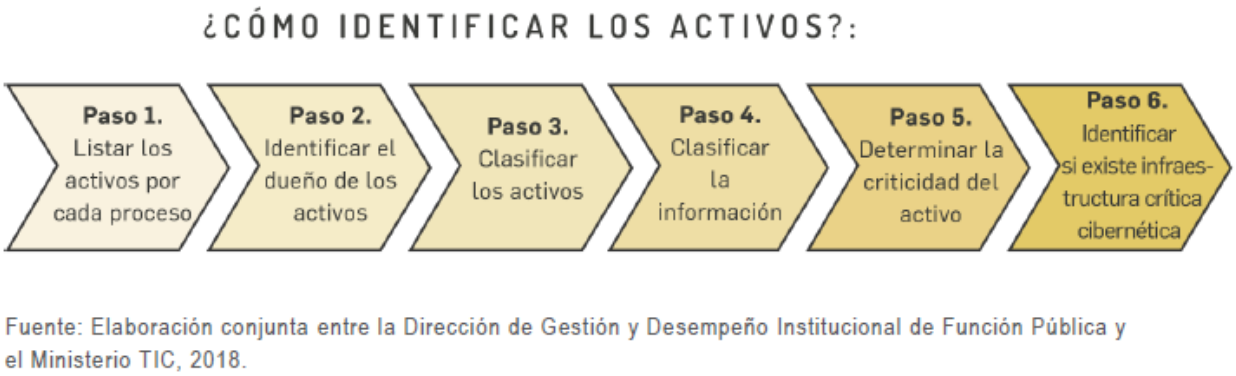
"Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control del IMP, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos" (DAFP, 2022).

Se aplican las siguientes fases

Fuente: *Guía para la administración del riesgo VS. 6- noviembre 2022- DAFP*

- Para los riesgos de Seguridad de la Información, como primer paso para la identificación de riesgos es necesario identificar los activos de información del proceso, a través de los siguientes pasos:

Identificación activos del proceso



Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

Tipología de Activos

TIPO DE ACTIVO	DESCRIPCIÓN
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
Intangibles	Aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el goodwill, entre otros.

Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

CRITERIOS DE EVALUACIÓN DE CRITICIDAD

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1: Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2: Niveles de Clasificación

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

Tabla3. Esquema de clasificación por confidencialidad

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

Tabla4. Esquema de clasificación por Integridad

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

Tabla5. Esquema de clasificación por Disponibilidad

Es de resaltar, que solamente se podrá identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

Pérdida de la confidencialidad
Pérdida de la integridad
Pérdida de la disponibilidad

“Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización” (DAFP, 2022).

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.

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.

Ahora bien, para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de gestión fiscal en las que potencialmente se genera riesgo fiscal) y circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la

causa principal del riesgo fiscal). Para este taller, puede usar las siguientes preguntas orientadoras

Tabla 11 Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.
Circunstancias inmediatas	En un ejercicio autocrítico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo1), son aplicables a la entidad?

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

7.1.1.1. CLASIFICACIÓN DEL RIESGO

Criterios de clasificación del riesgo

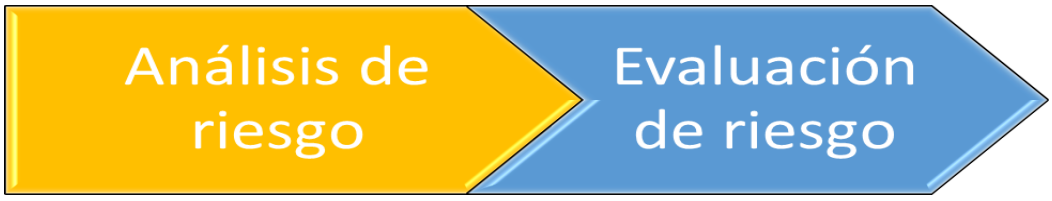
CLASIFICACIÓN	DESCRIPCIÓN	INTERRELACIÓN CON EL FACTOR DE RIESGO
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	Procesos
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	Evento externo
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.	Talento Humano
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	Tecnología
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.	Puede asociarse a varios factores
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.	Puede asociarse a varios factores
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres	❖ Infraestructura ❖ Evento externo

CLASIFICACIÓN	DESCRIPCIÓN	INTERRELACIÓN CON EL FACTOR DE RIESGO
	naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.	
Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.	Procesos
Seguridad de la Información	Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.	Tecnología

Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

7.1.2. VALORACIÓN DEL RIESGO

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona del riesgo inicial (RIESGO INHERENTE), para ello se desarrollará dos elementos:



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

7.1.2.1. ANÁLISIS DE RIESGO

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y susconsecuencias o impacto. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Por lo tanto, para calificar el riesgo se utilizará los siguientes criterios:

Determinar la probabilidad.

Actividades relacionadas con la gestión en entidades públicas

ACTIVIDAD	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD FRENTE AL RIESGO
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería. *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

- ***Criterio para definir el nivel de probabilidad***

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

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

- **Determinar el impacto**

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

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

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

IMPORTANTE: Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

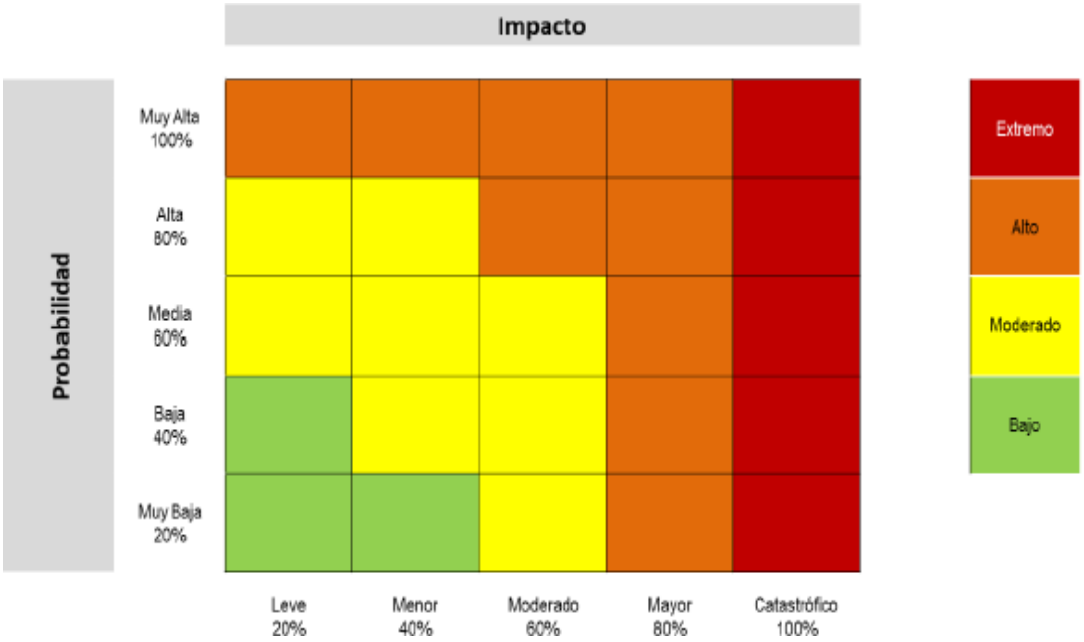
7.1.2.2. EVALUACIÓN DE RIESGO

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

- **Análisis preliminar (riesgo inherente):**

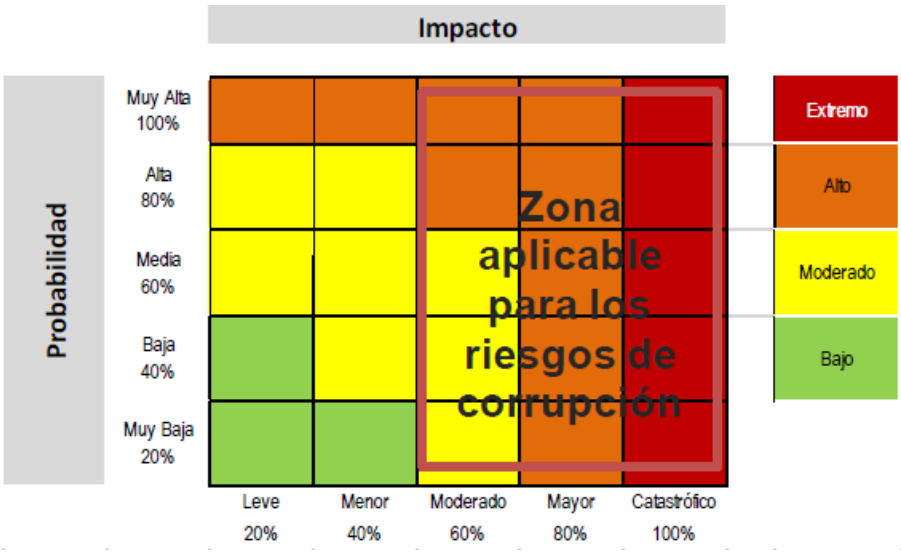
Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto, de acuerdo con la Matriz de calor que se relaciona a continuación:

Matriz de calor (niveles de severidad del riesgo)



Fuente: Guía para la administración del riesgo y el diseño de controles en entidadespúblicas, 2020

MATRIZ DE CALOR RIESGOS DE CORRUPCIÓN (NIVELES DE SEVERIDAD DEL RIESGO)



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

7.1.2.3. Valoración de controles

Para la valoración de controles se debe tener en cuenta:

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

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

- La metodología para valoración de los controles de riesgos de gestión, así como de seguridad de la información, es aplicable a la gestión del riesgo de corrupción.

Estructura para la descripción del control

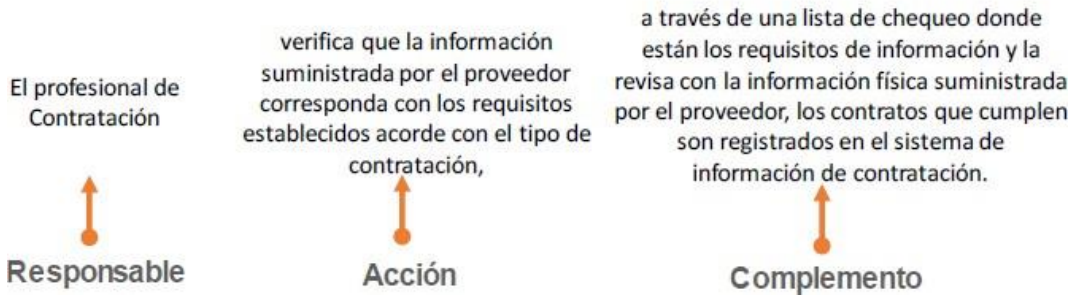
Componentes para la descripción de controles

CRITERIO	DESCRIPCIÓN
Responsable de ejecutar el control	Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
Acción	Se determina mediante verbos que indican la acción que deben realizar como parte del control.
Complemento	Corresponde a los detalles que permiten identificar claramente el objeto del control.

Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

Ejemplo redacción de control

Figura 15 Ejemplo aplicado bajo la estructura propuesta para la redacción del control



Fuente: Guía para la administración del Riesgo, 2020

TIPOLOGÍA DE CONTROLES Y LOS PROCESOS

TIPOLOGIA	DESCRIPCIÓN	MOVIMIENTO EN LA MATRIZ DE CALOR
Control preventivo	Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.	Atacan probabilidad
Control Detectivo	Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.	Ataca probabilidad

TIPOLOGIA	DESCRIPCIÓN	MOVIMIENTO EN LA MATRIZ DE CALOR
Control correctivo	Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.	Atacan impacto
Control manual	Controles que son ejecutados por personas.	Ataca probabilidad
Control automático	Son ejecutados por un sistema.	Ataca probabilidad

Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

Análisis y evaluación de los controles – Atributos:

Criterios evaluación de los controles

CARACTERISTICAS			DESCRIPCIÓN	PESO
		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.	15%

Atributos de eficiencia	Tipo		Se pueden generar reprocesos.	
		Correctivo	Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%

CARACTERISTICAS			DESCRIPCIÓN	PESO
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se real iza la actividad que con lleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que con lleva el riesgo.	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

7.1.2.4. NIVEL RIESGO RESIDUAL

El riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control, como se ilustra a continuación:

Figura 11. *Aplicación de controles para establecer el riesgo residual*

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

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

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

7.1.3. ESTRATEGIAS PARA COMBATIR EL RIESGO

Corresponde a la decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar.

Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

- **La aceptación del riesgo:** puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

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

- **Reducir el riesgo:** El nivel de riesgo debería ser administrado mediante el establecimiento de controles (mitigar), de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad o transferir parte del riesgo a través de seguros y tercerización.

Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

Nivel de aceptación y tratamiento del riesgo

COLOR	*ZONA DE RIESGO*	*TRATAMIENTO DEL RIESGO*	*PERIODICIDAD PARA EL SEGUIMIENTO*
	ZONA RIESGO EXTREMA	*Reducir el riesgo, evitar, compartir o transferir.*	*Trimestral*
	ZONA RIESGO ALTA	*Reducir el riesgo, evitar, compartir o transferir.*	
	ZONA RIESGO MODERADA	*Asumir el riesgo, reducir el riesgo.*	*Semestral*
	ZONA RIESGO BAJA	*Asumir el riesgo.*	*Anual*

Fuente: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP*

Importante: Los niveles de aceptación del riesgo:

- Puede ocurrir sin tratamiento de riesgo
- Los riesgos aceptados están sujetos a monitoreo
- Los riesgos de corrupción son inaceptables, siempre deben conducir a un tratamiento.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique:

- Responsable
- Fecha implementación
- Fecha seguimiento
- Estado

Nota: En caso de que se detecte que un riesgo se materialice, se considera que los controles no fueron efectivos y, por lo tanto, los líderes de los procesos deben reevaluar el riesgo e implementar nuevos controles.

Control de cambios

Versión	Fecha	Descripción Modificación
V.01	06/05/2021	Se crea la Política de Administración de Riesgos del IMP
V.02	23/12/2023	Se incluyen los riesgos fiscales y riesgos de seguridad de la información, establecidos en la "**Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP"**

ANDRES FELIPE VANEGAS CARDONA
Director General

GUILLERMO ANDRES GARCIA MORENO
Subdirector General de Planeación

Fuentes: *Guía para la administración del riesgo vs. 6- noviembre 2022- DAFP-Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas. Min TIC*