COLOMBIA POTENCIA DE LA VIDA

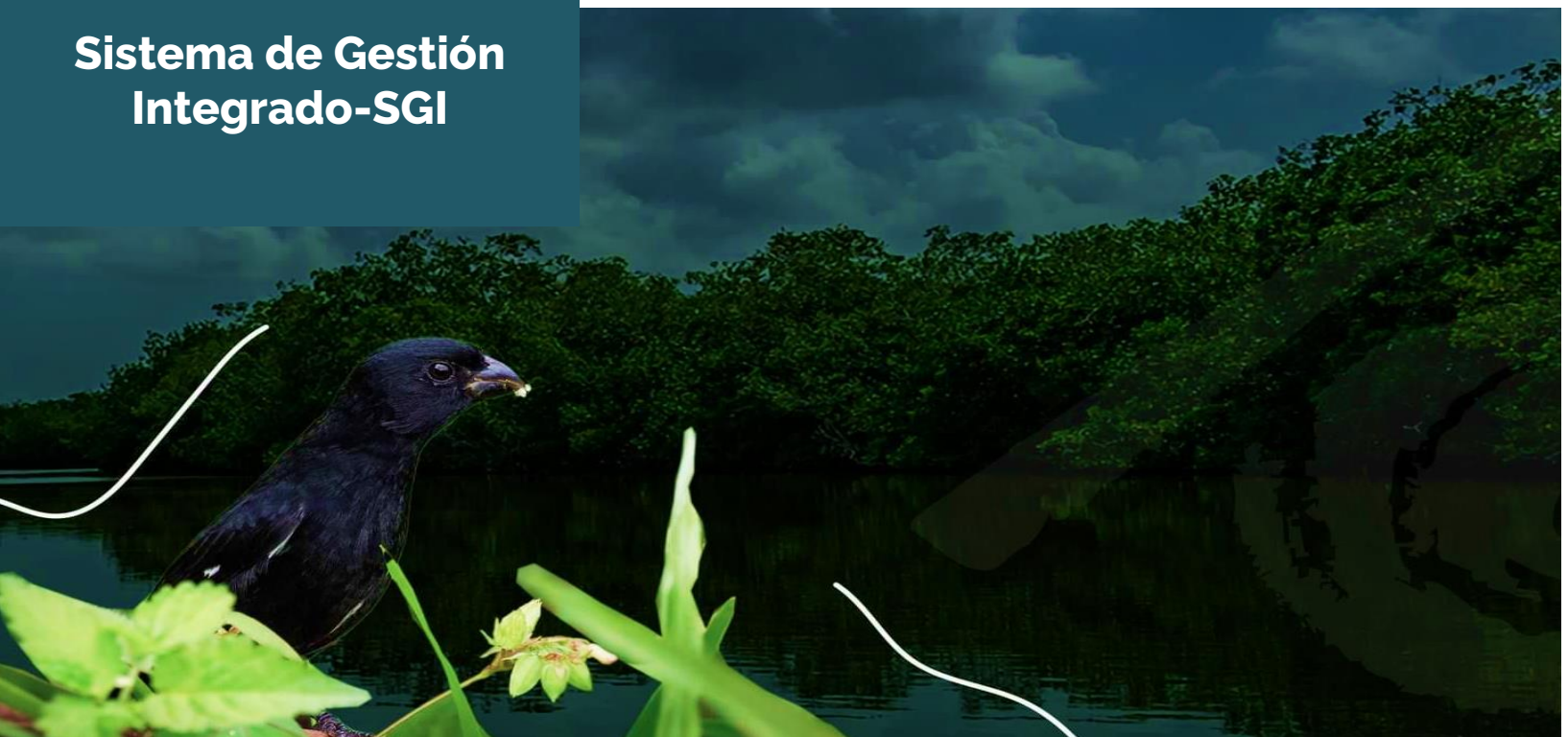
IDEAM
Instituto de Hidrología, Meteorología y Estudios Ambientales

Guía metodológica para la Gestión del Riesgo

Versión 6

CÓDIGO: E-SGI-G003
Fecha: 11/07/2023

Sistema de Gestión Integrado-SGI



Índice de contenido

Índice de Ilustraciones

Índice de Tablas

1. Desarrollo

La gestión de riesgos propende por identificar y mitigar la ocurrencia de desviaciones que afecten la misión, visión y los objetivos estratégicos y de proceso del Instituto de Hidrología, Meteorología y Estudios Ambientales (Ideam). Por lo anterior, se han definido los elementos para la administración de riesgos con base en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas", del Departamento Administrativo de la Función Pública-DAFP-

1.1 Objetivo

Establecer un esquema para ejercer una correcta y eficiente administración de los riesgos del Instituto, mediante la implementación de políticas, procedimientos y controles que permitan mitigar la probabilidad de ocurrencia de los eventos que afecten los objetivos estratégicos institucionales. Como consecuencia, dicho esquema de acciones se debe orientar hacia la calidad de los procesos y la eficiencia de sus servidores para apoyar la toma de decisiones por parte de la alta dirección.

1.2 Alcance

Abarca tanto los procesos definidos en el "Modelo de gestión por procesos" como las tareas desarrolladas por los servidores públicos que hacen parte de las sedes central, aeropuertos, estaciones y áreas operativas del Ideam. Incluye la identificación de los riesgos de gestión, corrupción y de operaciones estadísticas y estratégicas; la seguridad digital operativa o de gestión; así mismo como los riesgos fiscales. Abarca la identificación, el análisis, la valoración, el tratamiento y monitoreo por parte de la Oficina Asesora de Planeación y el seguimiento de riesgos por parte de Control Interno.

1.3 Política de administración del riesgo

El Instituto de hidrología meteorología y estudios ambientales-Ideam, en cumplimiento a su misionalidad, se compromete con sus grupos de valor y de interés a establecer medidas y herramientas encaminadas a controlar los efectos, mitigar su impacto y aprovechar las oportunidades para mejorar la eficacia del Sistema de Gestión Integrado-SGI, para de esta manera, responder a los acontecimientos y potenciales acciones de riesgos de corrupción, de gestión, fiscales y de seguridad de la información (para activos con nivel crítico y de conservación digital) que puedan afectar el desempeño de sus procesos y el logro de sus objetivos institucionales

Por lo anterior, la Alta Dirección vela por la administración integral del riesgo, fomentando la participación de los servidores públicos y demás colaboradores, propiciando procesos permanentes de comunicación, revisión, seguimiento y control a las acciones de mejora para el tratamiento de los riesgos y potencializar las oportunidades

Además, teniendo en cuenta que la estructura de la entidad es dinámica en el tiempo,

los instrumentos diseñados para la administración del riesgo son susceptibles de mejora y serán revisados continuamente para ello, la descripción, actualización, monitoreo y seguimiento los cuales podrán ser consultados en la página web de la entidad, conforme a la política transparencia y acceso a la información pública del MIPG.

1.4 Marco normativo

La gestión de los riesgos en el Instituto se enmarca en el siguiente conjunto de normas que rigen la administración del riesgo como apoyo al buen gobierno corporativo y mejores medidas de control en las entidades.

Constitución Política de Colombia de 1991, artículo 209. La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.

Constitución Política de Colombia, artículo 269. En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas.

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 489 de 1998. Estatuto Básico de Organización y funcionamiento de la administración pública.

Decreto 2145 de 1999. Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y territorial y se dictan otras disposiciones. Modificado parcialmente por el Decreto 2593 del 2000.

Directiva Presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.

Decreto 1537 de 2001. Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado.

Ley 872 de 2003. Establece el Sistema de Gestión de la Calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios.

Decreto 943 de 2014. Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).

Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

NTCPE 1000 2017.Norma Técnica de la Calidad del Proceso Estadístico. Requisitos de Calidad para la Generación de Estadísticas. DANE-ICONTEC.

NTCPE 1000-2020. Norma Técnica de la Calidad del Proceso Estadístico. Requisitos de Calidad para la Generación de estadísticas. DANE-ICONTEC.

1.5 Términos y definiciones[1]

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 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 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).

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).

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.

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

Recurso público: Para efectos del capítulo de riesgos fiscales, 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,

[1] Tomado de " *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas versión 6 "*

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

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

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; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C- 340-07).

Oportunidades: Riesgos positivos, entendidos como oportunidades externas o fortalezas internas que permiten orientar y alinear los riesgos con los objetivos estratégicos y dar cumplimiento a la normatividad legal vigente

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.

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. 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 riesg
o. 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.

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.

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales.

Control: Medida que permite reducir o mitigar un riesgo.

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.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados Integridad: Propiedad de exactitud y completitud.

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

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

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.

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.

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.

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.

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.

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.

Modelo Integrado de Planeación y Gestión: El MIPG es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.

1.6 Roles y responsabilidades

De conformidad a lo establecido en el Modelo Integrado de Planeación y Gestión -MIPG, a continuación, se relacionan las políticas y líneas de defensa con sus correspondientes niveles de responsabilidad y autoridad establecidos para la administración del riesgo, buscando una adecuada gestión y prevención de la materialización de estos.

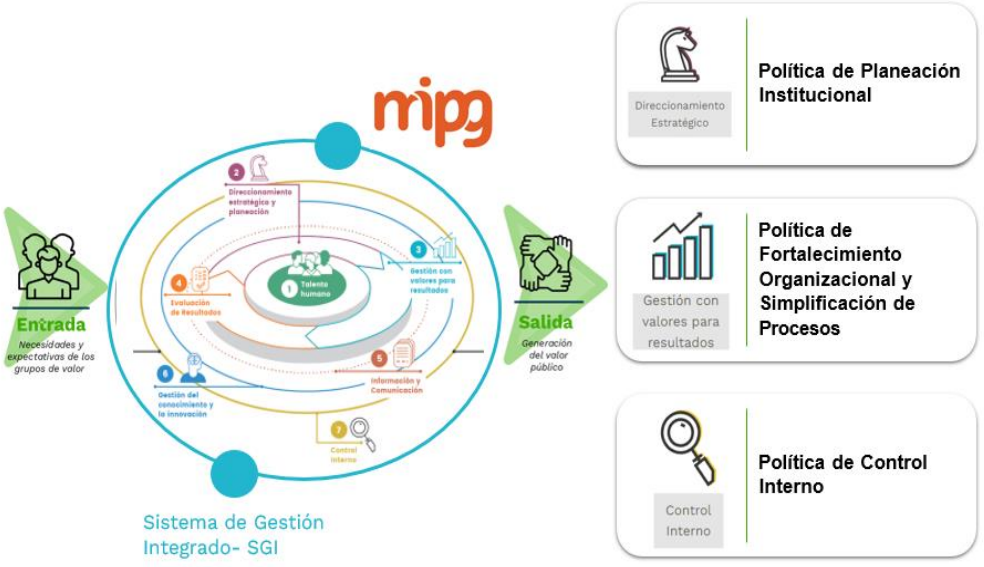


Ilustración 1 Alineación riesgos con el Modelo Integrado de Planeación y Gestión-MIPG

Los roles y las responsabilidades en la gestión del riesgo son de carácter integral y diferenciado, y participan todos los niveles de la gestión institucional. De esta manera se asegura el logro, anticipándose y minimizando los riesgos que pueden afectar a la entidad. Esta gestión se desarrolla mediante las líneas de defensa estratégica y de responsabilidad de la gestión del riesgo y control.

Tabla 1 Líneas de defensa en el Modelo Estándar de Control Interno, Fuente: Manual operativo MIPG, marzo, 2021.

Línea de defensa	Conformada por	Funciones frente a la gestión del riesgo
Línea de defensa estratégica	Dirección general, Comité Institucional de Control Interno, Comité Institucional de Gestión y Desempeño	• Emitir, revisar, validar y supervisar el cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad. • Establecer las directrices para la identificación, análisis, valoración de riesgos y oportunidades en el desarrollo de los objetivos y metas institucionales. • Fortalecer el Comité Institucional de Coordinación de Control Interno, incrementando su periodicidad para las reuniones. • Evaluar el funcionamiento del Esquema de Líneas de Defensa, incluyendo la línea estratégica. • Definir líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. • Definir y evaluar la "Política de administración del riesgo". La evaluación debe considerar su aplicación en la entidad, los cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. • Evaluar la política de gestión estratégica del talento humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar).

Línea de defensa	Conformada por	Funciones frente a la gestión del riesgo
Primera línea de defensa	Servidores en sus diferentes niveles, líderes o responsables de proceso	• Mantener controles internos efectivos; por consiguiente, • identificar, evaluar, controlar y mitigar los riesgos. Aspectos que debe tener en cuenta la línea de defensa: • El conocimiento y la apropiación de políticas, procedimientos, manuales, protocolos y otras herramientas que faciliten tomar acciones para el autocontrol en sus puestos de trabajo. • La identificación de riesgos y el establecimiento de controles, así como el seguimiento, acorde con su diseño, con el fin de evitar la materialización de estos. • El seguimiento a los indicadores de gestión institucionales y de los procesos, según corresponda. • La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. • La coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la segunda línea de defensa.
Segunda línea de defensa	Jefe de Oficina Asesora de Planeación, líderes o coordinadores de contratación, financiera y de TIC	• Asegurar los controles y procesos de gestión del riesgo de la primera línea de defensa para que sean apropiados y funcionen correctamente. • Asesorar y acompañar a los procesos y/o dependencias en la implementación de la gestión del riesgo y oportunidades como insumo fundamental de la planificación institucional tanto estratégica como operativa, tanto como de su mejoramiento continuo. • Supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas para adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos. • Asegurar que los controles y procesos de gestión del riesgo de la primera línea de defensa sean apropiados y funcionen correctamente. Supervisar la implementación eficaz de prácticas de gestión de riesgo. • Consolidar y analizar la información sobre temas fundamentales para la entidad, como base para tomar decisiones y acciones preventivas necesarias que eviten materializaciones de riesgos. • Trabajar junto a las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno. • Asesorar a la primera línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos. • Establecer los mecanismos para la autoevaluación

Línea de defensa	Conformada por	Funciones frente a la gestión del riesgo
		requerida: auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora.
Tercera línea de defensa	Oficina de Control Interno	• Evaluar de manera independiente y objetiva los controles de segunda línea de defensa para asegurar su efectividad y cobertura; así mismo, evaluar los controles de primera línea de defensa que no se encuentren cubiertos y los que inadecuadamente son cubiertos por la segunda línea de defensa. • A través de su rol de asesoría, dar orientación técnica y hacer recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces, con enfoque hacia el cumplimento efectivo de los objetivos. • Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. • Asesorar proactiva y estratégicamente a la Alta Dirección y a 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. • Informar los hallazgos y proporcionar recomendaciones de • forma independiente.

1.7 Contexto de la organización

El inicio en la administración de los riesgos está dado por la identificación del contexto, normatividad, planes y programas que se desarrollan en el marco de la plataforma estratégica de la entidad. El contexto de la organización comprende la estructura institucional, cultura organizacional, objetivos del proceso, procedimientos relacionados, sistemas de información, recursos humanos y económicos con respecto a condiciones externas económicas, sociales, culturales, políticas, legales, ambientales o tecnológicas que inciden en su gestión. Comprender el contexto permite conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

Para priorizar la identificación y gestión de riesgos será necesario analizar los posibles eventos que puedan afectar el logro de los objetivos estratégicos y de sus procesos, para lo cual se deberá diligenciar el formato **E-SIG-F024_Contexto_Estratégico**

1.8 Objetivos de proceso

El objetivo del proceso debe dar respuesta a los interrogantes: qué, cómo, para qué, cuando

y cuánto. La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión, la visión institucional, y los objetivos de procesos.

1.9 Matriz de riesgos

El formato E-SGI-F006 "mapa de riesgos" es la herramienta que el instituto definió en su Sistema de Gestión para consignar la información que da cuenta del desarrollo de cada una de las etapas de la presente metodología, y en la que los líderes de proceso deben diligenciar o actualizar el mapa, de acuerdo con las indicaciones y lineamientos definidos en esta *Guía*. Todo lo anterior, con la asesoría y revisión de la Oficina Asesora de Planeación, y a partir de las orientaciones metodológicas establecidas en las guías o herramientas dispuestas para tal fin por el Departamento Administrativo de la Función Pública (DAFP), la Secretaría de Transparencia de la Presidencia de la República y las que puedan ser aplicables en lo que concierne a la administración de riesgos, acorde a la dinámica y necesidades de la entidad.

1.10 Descripción de metodología administración de riesgos

El IDEAM como Entidad pública ha estructurado la metodología para el desarrollo y cumplimiento de su Política Integral para la Administración del Riesgo a partir de los lineamientos que en esta materia ha impartido el Departamento Administrativo de la Función Pública mediante la Guía para la administración del riesgo y el diseño de controles en entidades públicas en la versión vigente. De esta manera la Entidad adopta en su totalidad estos lineamientos a las necesidades particulares y contexto propio de la Entidad y define los pasos necesarios para llevar a cabo la gestión de los riesgos de manera efectiva.

Es importante tener en cuenta que la DAFP establece los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de gestión, corrupción, de seguridad y de la información y fiscales, así mismo, una metodología y redacción diferente, por lo tanto, deberá remitirse al numeral correspondiente para garantizar la correcta identificación y estructuración del riesgo dependiendo de su tipología.

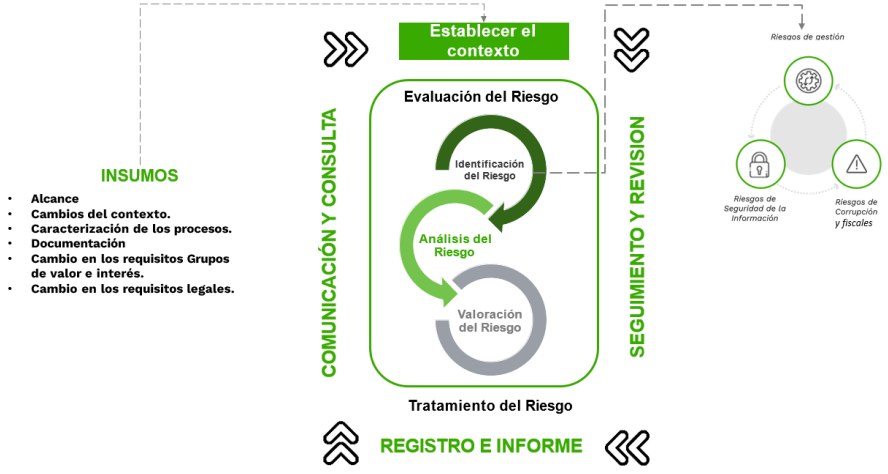


Ilustración 2 Ciclo de Administración de riesgos

- **Antes de iniciar la metodología:**

De acuerdo con Modelo Integrado de Planeación y Gestión - MIPG, en su "política de planeación institucional" cuyo propósito es permitir que la entidad defina su ruta estratégica y operativa que guiará su gestión, con miras a satisfacer las necesidades de sus grupos de valor.

Es por ello por lo que la identificación y valoración de riesgos debe estar articulada al desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos.

En ese sentido, es importante conocer y analizar previamente la información relacionada con la entidad en cuanto a:

- Misión y la Visión de la entidad.
- Planeación Institucional.
- Objetivos Estratégicos.
- Mapa o Red de Procesos del SIG.
- Activos de Información.
- Aspectos e impactos Ambientales.

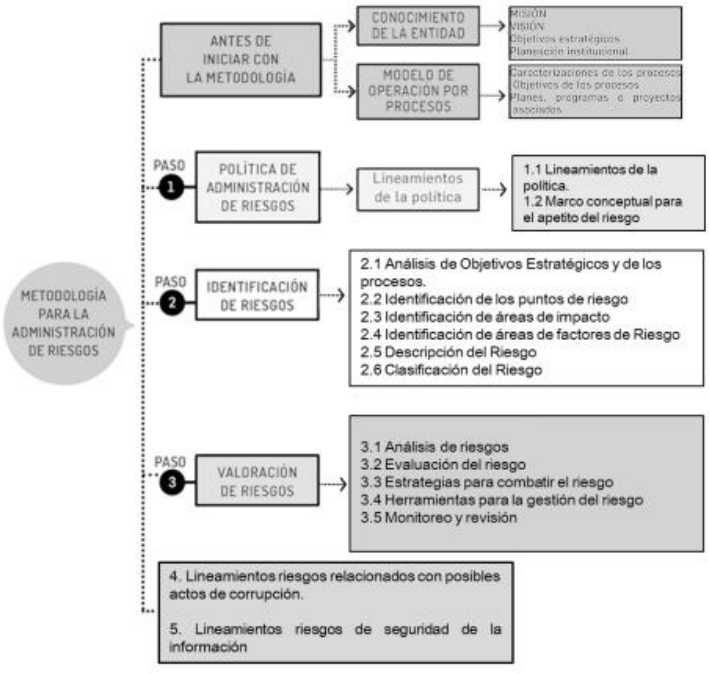


Ilustración 3 Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos, planeación institucional, entre otros aspectos, permitiendo conocer y entender la entidad, y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

La estructura de la metodología aplicada para la administración de riesgos en el formato de riesgos E-SGI-F006 "mapa de riesgos" se establece de la siguiente manera:

1.10.1 RIESGOS DE GESTIÓN

Identificación del riesgo

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, teniendo en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

- **Análisis de los objetivos:**

Para la correcta identificación del riesgo, es fundamental realizar un análisis sobre los objetivos estratégicos y los objetivos del proceso.

- **Identificación de puntos de riesgo:**

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo, para la identificación de este punto se podrán verificar las caracterizaciones del proceso los cuales permiten evidenciar las actividades que pueden ser fuente potencial del riesgo en el Planear, Hacer, Verificar y Actuar.

Además, para identificar estos puntos de riesgo es importante tener en cuenta la documentación del proceso como procedimientos, guías, protocolos, manuales, instructivos, documentos soporte y formatos, entre otros. Así como, la cadena de valor público, desde insumos, procesos, productos, resultados, efectos e impactos y el cumplimiento de los objetivos.

- **Factores de riesgo**

Son las fuentes generadoras de riesgos, las cuales se documentan en los contextos estratégicos por proceso, corresponde a la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. (NTC ISO 31000, Numeral 2.9).

En la siguiente tabla se describen los factores de riesgo con los que se realizará dicha identificación en la entidad:

Tabla 2 Descripción de factores de riesgo

Factor	Definición	Descripción
Procesos 	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Corresponde a los riesgos o posibilidad de ocurrencia que afecten los procesos de la entidad, provenientes del funcionamiento y operatividad de los sistemas de información, de la estructura de la entidad y de la articulación interdependencias. Falta de procedimientos, errores de grabación, autorización, errores en cálculos para pagos internos y externos Falta de capacitación, temas relacionados con el personal.
Talento humano 	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurtos activos, posibles comportamientos no éticos de los empleados, fraude interno (corrupción, soborno). Se asocia al uso del poder para desviar la gestión de lo público hacia el beneficio privado.
Tecnología 	Eventos relacionados con la infraestructura tecnológica de la entidad.	Están relacionados con el uso de la tecnología en la entidad para satisfacer sus necesidades actuales y futuras, y el cumplimiento de la misión. Daño de equipos, caída de aplicaciones, caída de redes, errores en programas.
Infraestructura 	Eventos relacionados con la infraestructura física de la entidad	Aquellos riesgos o posibilidades de ocurrencia de afectación a los bienes, entre otros que perjudiquen la sostenibilidad del Instituto. Derrumbes, incendios, inundaciones, daños a activos fijos.
Evento externo 	Situaciones externas que afectan la entidad.	Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de los objetivos institucionales y afectar la autonomía, principios e integridad de la entidad. Incluye aspectos relacionados con el ambiente físico y digital, y con las personas. Suplantación de identidad, asalto a la oficina Atentados, vandalismo, orden público

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6

Los factores relacionados podrán actualizarse según se considere necesario, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, y se incluyen como tema clave dentro de los lineamientos de la política de administración del riesgo:

Tabla 3 Riesgos Operaciones Estadísticas

Tipo	Descripción
Operaciones estadísticas	Se asocian a los riesgos que se identifican en el cumplimiento e implementación de la NTCPE 1000 2017. "Norma técnica de la calidad del proceso estadístico". Requisitos de calidad para la generación de estadísticas. DANE-ICONTEC NTCPE 1000-2020. "Norma técnica de la calidad del proceso estadístico". Requisitos de calidad para la generación de estadísticas. DANE-ICONTEC.

Fuente: NTCPE 1000 2017

Descripción del riesgo:

La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento, tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad, iniciando con la con la frase **posibilidad de** y seguido del impacto en la palabra "afectación económica" o "afectación reputacional" según se haya definido previamente.

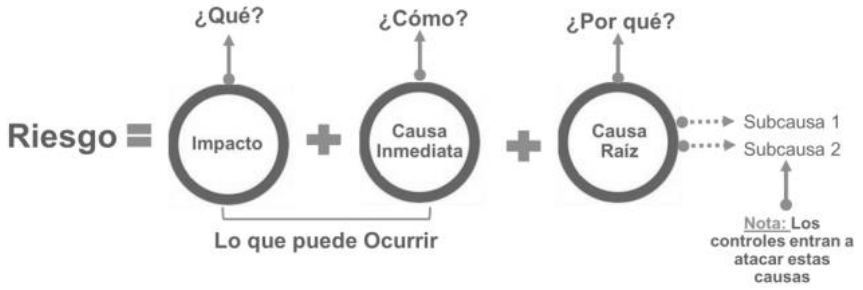


Ilustración 4.Redacción del riesgo

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6

La redacción descrita permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y su causa raíz, siendo esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

A continuación, se definen los elementos claves para la redacción del riesgo:

- **Impacto:** Análisis de las consecuencias que puede ocasionar a la organización, la materialización del riesgo, en términos de afectación de la reputación, afectación económica o ambas.
- **Causas inmediatas**: Son aquellos factores que generan el riesgo; por ejemplo, falta de procedimientos, falta de capacitación, daño de equipos, caída de redes y daños a activos fijos, entre otros.
- **Causa raíz:** Es la causa principal que origina el riesgo. Los controles se orientarán a mitigar esta causa.

Ejemplo de redacción de riesgo:

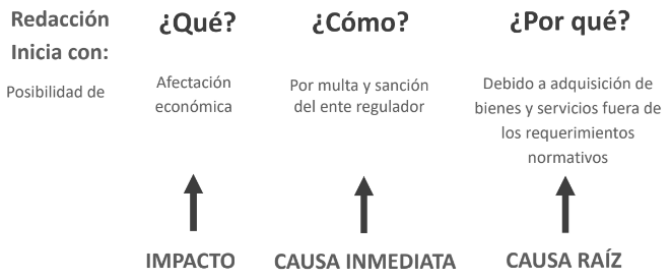


Ilustración 5. Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo.

Fuente: Guía Para Para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2022.

Clasificación del riesgo

Una vez definidos los factores de riesgo se realizará clasificación de los tipos riesgos definidos, lo cual permite agrupar los riesgos identificados, se clasifica cada uno de los factores de riesgos en los siguientes tipos:

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

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

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

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

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

Tabla 4 Clasificación del Riesgo

TIPO DEL RIESGO	FACTORES DE RIESGO

Ejecución y Administración de Procesos	Procesos
Fraude externo	Evento externo
Fraude interno	Talento humano
Fallas tecnológicas	Tecnología
Relaciones laborales	Pueden asociarse a varios factores
Usuarios, productos y prácticas	Pueden asociarse a varios factores
Daños a activos fijos	Infraestructura

Fuente: Guía Para Para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2022.

Valoración del Riesgo:

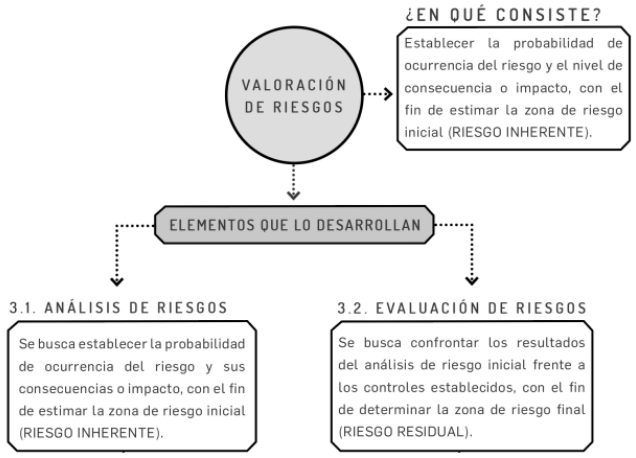


Ilustración 6 Valoración del riesgo

Fuente: Guía Para Para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2022

Se desarrolla a partir de las siguientes fases:

- **Análisis de Riesgos:**
  - Determinar la Probabilidad
  - Determinar el Impacto
- **Evaluación de Riesgos:**
  - Análisis Preliminar (Riesgo Inherente)
  - Valoración de Controles
  - Estructura para la descripción del control
  - Tipología de controles y los procesos
  - Análisis y evaluación de controles – Atributos
  - Nivel de Riesgo (Riesgo Residual)
- **Estrategias para Combatir el Riesgo:**
  - Tratamiento del Riesgo

- **Herramientas para la Gestión del Riesgo:**
  - Gestión de Eventos – Riesgos Materializados

- Indicadores Clave de Riesgos

- **Monitoreo y Revisión de los Riesgos**

Análisis del riesgo

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

- **Determinar la Probabilidad:** Se busca establecer la probabilidad y el impacto. Puesto, en otros términos, lo que generará como resultado el riesgo residual. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año, lo cual establece determinar la frecuencia con la que se lleva a cabo una actividad.

  Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad

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

Ilustración 7 Criterios de probabilidad

. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6.

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al **número de veces que se pasa por el punto de riesgo en el periodo de 1 año**, en la siguiente tabla se establecen los criterios para definir el nivel de probabilidad:

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

Tabla 5 Criterios para definir la probabilidad,

Determinar el Impacto:

	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%

Para la construcción de la tabla de criterios se definen los **impactos económicos y reputacionales como las variables principales**. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

Ejemplo:

Para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, **se tomará el más alto**, en este caso sería el nivel moderado. Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Tabla 6 Criterios para definir el impacto

	Afectación Económica (o	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna 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 provedores
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 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 publicitarios sostenible a nivel país

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

Evaluación de riesgos

A partir del análisis de la probabilidad y sus consecuencias, se establece la zona de riesgo inherente. El riesgo inherente se ubica en 4 zonas de severidad: **bajo, moderado, alto y extremo.**

- **Riesgo INHERENTE o antes de controles:**

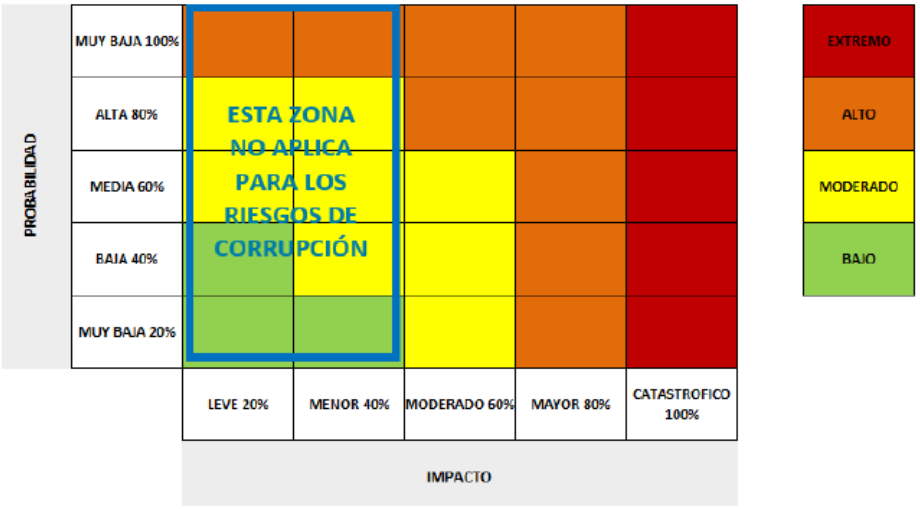


Ilustración 8. Mapa de calor riesgo inherente

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

Ejemplo:

Proceso: *Gestión de recursos*
Objetivo: *Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación*
Riesgo identificado: *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 = *Media 60%*
Impacto Inherente: *Mayor 80%*

Aplicando el mapa de calor tenemos:

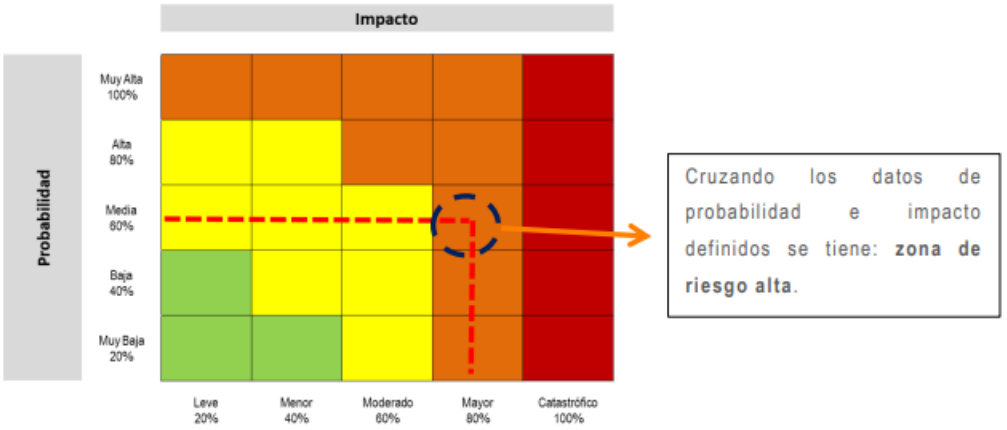


Ilustración 9 Mapa de Calor ejemplo

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

El mapa de calor permite visualizar los riesgos en las zonas definidas (bajo, moderado, alto y extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a aceptar (apetito del riesgo) en función del impacto de estos en la Entidad.

- **Apetito al riesgo**: El apetito al riesgo será definido por cada proceso de acuerdo con el nivel de impacto que genere su materialización. En general, se aceptan los riesgos cuyo nivel de riesgo final sea bajo e incluya controles de prevención, detección y corrección.

- **Tolerancia al riesgo**: La tolerancia al riesgo se define en cada proceso de acuerdo con los porcentajes de desviación máxima identificados. La tolerancia a los riesgos de gestión, estratégicos y de seguridad digital se califica con nivel alto cuando la valoración esté determinada por el impacto, no por la probabilidad. En riesgos de corrupción no aplica el apetito ni la tolerancia al riesgo.

La evaluación del riesgo se realiza de acuerdo con los resultados que se obtengan en la matriz, teniendo en cuenta la valoración del riesgo residual:

- Si el riesgo de gestión se ubica en la zona de riesgo **baja** la entidad puede asumirlo, esto debido a que se encuentra en un nivel en el que puede ser controlado sin necesidad de tomar medidas adicionales a las establecidas.
- Si el riesgo se ubica en las zonas **moderada** o **alta,** se deben tomar medidas de control adicionales a las actuales que conduzcan a disminuir la probabilidad o la consecuencia o ambas. En lo posible, los riesgos se deben llevar a la zona baja.
- Si el riesgo se ubica en la zona de riesgo **extrema**, se deben eliminar las causas que generan el riesgo e implementar controles preventivos para evitar la probabilidad de ocurrencia y disminuir el impacto.

Valoración de controles

Se busca confrontar los resultados del análisis del riesgo inicial (INHERENTE) frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RESIDUAL).

Riesgo inicial (Inherente) – Efecto de los controles = Riesgo Final (Residual)

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo. Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

Estructura para la descripción del control:

Los controles orientados a atacar la causa raíz para prevenir la materialización del riesgo tienen en cuenta que cada líder de proceso o su representante deben definir, implementar y monitorear los controles establecidos.

Para establecer el control se tendrá en cuenta:

- La identificación del cargo que es responsable del control.
- La acción del control se redacta como verbo en infinitivo.
- El complemento o los detalles que identifican el objeto de control.

Se propone una adecuada redacción del control así:

Responsable+ Acción+ Complemento

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.

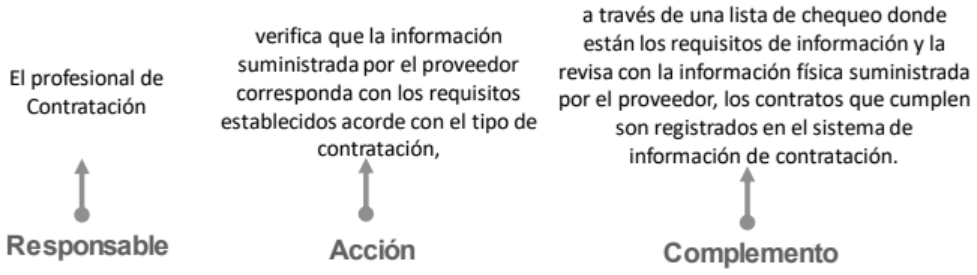


Ilustración 10. Ejemplo aplicado redacción del control.

Fuente: Guía Para La Administración del Riesgo el diseño de controles en entidades públicas versión 6

Qué hacer en caso de desviaciones: La redacción del control debe contemplar cuál es el manejo que se le da a las observaciones o desviaciones detectadas durante su ejecución.

Ejemplo: - Cuando se detecta que la documentación recibida está incompleta, se envía un correo electrónico solicitando la información faltante a la dependencia correspondiente. - Cuando se coteja en el sistema y los datos no coinciden, se envía un correo electrónico solicitando la revisión de la información por parte del profesional delegado.

Tipología de los controles:

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la siguiente ilustración se consideran 3 fases globales del ciclo de un proceso así:

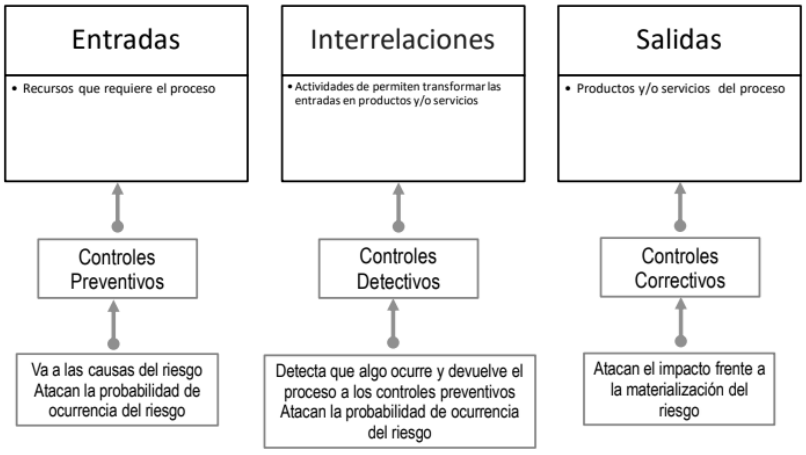


Ilustración 11 Tipología de Controles

Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6.

Tabla 7 Tipo de Controles

Tipo de control	Descripción	Forma de ejecución
Preventivo	Control establecido en la entrada del proceso y antes de que se realice la actividad originadora del riesgo.	Manual / automático
Detectivo	Se identifica durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.	Manual / automático
Correctivo	Control accionado en la salida del proceso y después de que se materializa el riesgo.	Manual / Automático

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

Así mismo, de acuerdo con la **forma** como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

Evidencia de ejecución:
Los controles deben relacionar la evidencia de su ejecución, la cual servirá de insumo para revisión por parte de terceros en la que se podría verificar lo siguiente:

- Fue ejecutado por el responsable designado.
- Se realizó de acuerdo con la periodicidad establecida.
- Se cumplió con el propósito del control.
- Se evidencia tratamiento a las desviaciones detectadas durante la ejecución del control.

Análisis y evaluación de los controles

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia e informativos. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

Tabla 8. Atributos de eficiencia e informativos del control

CARECTERÍSTICAS			DESCRIPCIÓN	PESO
Atributos de Eficiencia	Tipo	**Preventivo**	Va hacia las causas del riesgo, aseguran el resultado final esperado.	**25%**
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	**15%**
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	**10%**
	Implementación	**Automático**	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	**25%**

		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	**15%**
***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 realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	**Con Registro**	El control deja un registro que permite evidencia de la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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

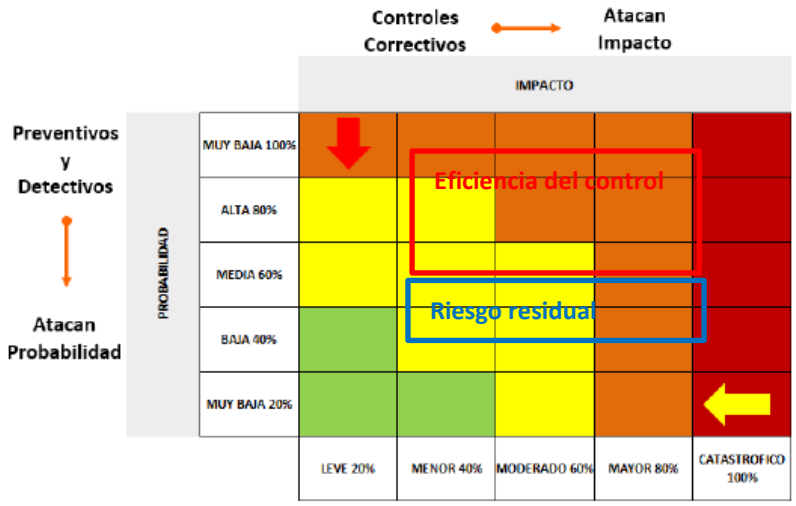
***Nota:** Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad, es importante resaltar que la actual metodología de evaluación de controles es más estricta, otorgando calificación solo a los atributos de eficiencia (tipo de control e Implementación).

Una vez se establecen los controles, se da un movimiento en los ejes de probabilidad o impacto, de acuerdo con el tipo de control aplicado. Los controles de preventivos y detectivo atacan la probabilidad de ocurrencia; y, los controles de correctivos atacan el impacto una vez se ha materializado el riesgo. En caso de no contar con controles de corrección, el impacto residual es el mismo calculado inicialmente. Es importante señalar que en este caso no será posible su movimiento en la matriz para el impacto.

Nivel del riesgo (riesgo residual)

El nivel de riesgo final es el resultado del movimiento en los ejes de acuerdo con el tipo de control aplicado.

Ilustración 12 Mapa de calor del riesgo residual



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

- **Estrategia para combatir el riesgo:**

Consiste en la decisión frente al nivel de riesgo final.

Reducir: Cuando se considera que el riesgo final es alto y se determina tratarlo mediante la mitigación (deducción del riesgo) no es necesario aplicar un control adicional, o la transferencia (tercerizar o trasladar el riesgo), en este la responsabilidad económica recae en el tercero, pero la responsabilidad reputacional no se transfiere.

Aceptar: Una vez analizado el nivel de riesgo se toma la decisión de asumirlo. Es decir, se asume cuando en el documento E-SGI-F006 "Matriz de riegos", la calificación del riesgo, posterior a la aplicación de controles es baja.

Evitar: Si se considera que el riesgo es muy alto se define no asumir la actividad que genera el riesgo.

Plan de tratamiento

El tratamiento de un riesgo está diseñado para combatir o mitigar el riesgo, las decisiones que se toman frente a un determinado nivel de riesgo, pueden ser **reducir, aceptar, y evitar**. Se deben analizar frente al Riesgo Residual.

El plan de tratamiento describe el modo en que se estructurarán y se llevarán a cabo las actividades complementarias a los controles en la administración de riesgos. Las acciones que se realizan para fortalecer los controles existentes pueden ser de dos tipos:

- Extremar un control existente (como por ejemplo aumentar la periodicidad de la aplicación de un control preestablecido).
- Implementar nuevas acciones (como por ejemplo nuevos formatos de control, checklist, reuniones periódicas de seguimiento con sus respectivas actas, entre otras). La aplicación de nuevas acciones no sustituye la obligatoriedad de la aplicación de los controles estandarizados.

Para que un tratamiento sea válido **se debe demostrar con evidencia objetiva que el tratamiento planteado está siendo ejecutado.**

Responsable: Define el líder, el apoyo y los miembros del equipo de gestión de riesgos para cada tipo de actividad del plan de gestión de los riesgos, y explica sus responsabilidades.
Cronograma de implementación de acciones: Se establecen las fechas de inicio y determinación para la implementación de las acciones de control. Estos seguimientos se deben hacer dependiendo del nivel de evaluación del riesgo.

1.10.2 RIESGOS DE CORRUPCIÓN

Identificación

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. Con el fin de facilitar la identificación de riesgos de corrupción y fraude y evitar que se confunda con un riesgo de gestión, se debe verificar si cumple con los siguientes criterios, estén se debe analizar y calificar a partir de las consecuencias identificadas en la descripción del riesgo:

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

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Ilustración 13 Matriz para la definición de riesgos de corrupción.
Fuente: Secretaría de Transparencia de la Presidencia de la República.

Teniendo en cuenta que los riesgos de corrupción son los efectos que cada hecho de corrupción (incertidumbre) que afectan la capacidad institucional de cumplir sus objetivos. Para la redacción de los riesgos de corrupción debe tenerse en cuenta:

- Debe estar directamente relacionado con el hecho de corrupción y estar expresado como el efecto que se produciría en relación con la capacidad de lograr los objetivos.
- Los hechos de corrupción son inaceptables.
- Los riesgos de corrupción son indeseables.
- El riesgo de corrupción debería tratar de evitarse, estableciendo controles para el hecho de corrupción.

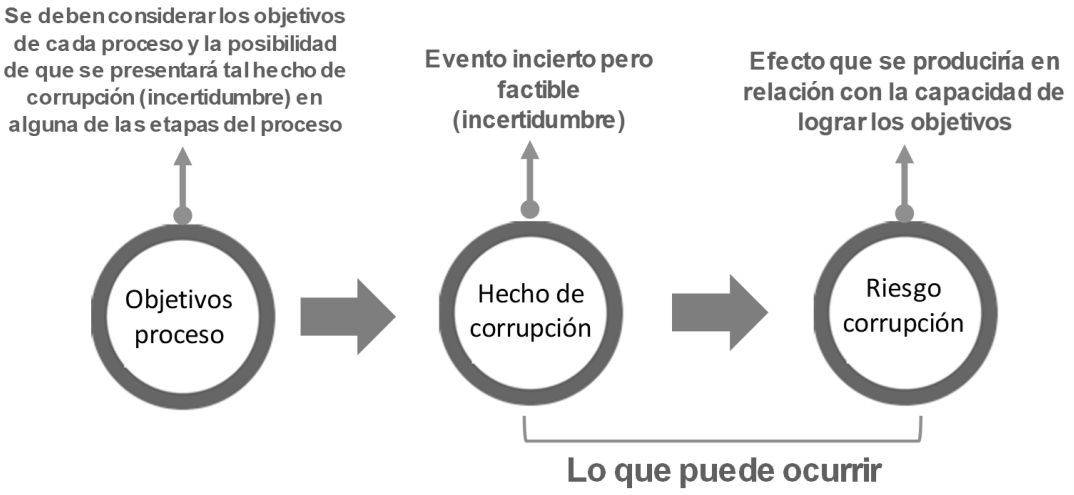


Ilustración 14 Estructura propuesta para la identificación del riesgo de corrupción, fuente DAFP

El Riesgo debe estar descrito de forma clara, de tal manera que se identifiquen los cuatro elementos que lo constituyen como un riesgo de corrupción. Su redacción no debe dar lugar a ambigüedades o confusiones.

Definición de impacto para riesgos de corrupción

A diferencia de los riesgos estratégicos, digitales y de gestión, el impacto de los riesgos de corrupción se valora por medio de las siguientes preguntas a partir de la respuesta Sí/No, posteriormente se cuenta el número de respuestas positivas y se verifica con la tabla de validación.

Tabla 9 Criterios para definir el impacto en riesgos de corrupción

Formato para determinar el impacto de los riesgos de corrupción				
Núm.	Factor	**Pregunta: si el riesgo de corrupción se materializa podría:**	**RESPUESTA**	
			Sí	**No**
1	Recursos	¿Generar pérdida de recursos económicos?		
2	Estrategia	¿Afectar el cumplimiento de misión de la entidad?		
3		¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
4		¿Afectar la generación de los productos o la prestación de servicios?		
5	Imagen/ reputación	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6		¿Generar pérdida de credibilidad del sector?		
7		¿Afectar la imagen?		
8		¿Afectar la imagen nacional?		
9	Ciudadanía	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
10		¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
11	Operacional/ organizacional	¿Afectar al grupo de funcionarios del proceso?		
12		¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
13	Legales	¿Generar intervención de los órganos de control, de la Fiscalía o de otro ente?		
14		¿Dar lugar a procesos sancionatorios?		
15		¿Dar lugar a procesos disciplinarios?		
16		¿Dar lugar a procesos fiscales?		
17	Información	¿Dar lugar a procesos penales?		
18		¿Generar pérdida de información de la entidad?		

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

El impacto de los riegos de corrupción se clasifica por el número de respuestas afirmativas (Sí), así:

Tabla 10 Definición del impacto en riesgos de corrupción por número de respuestas afirmativa

Impacto del riesgo	Número de respuestas afirmativas
Moderado	1 a 5 respuestas
Mayor	6 a 11 respuestas
Catastrófico	12 a 18 respuestas

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

Tratándose de riesgos de corrupción, el impacto siempre será negativo, es por ello que no aplica la identificación de riesgos bajos o leves.

1.10.3 RIESGO DE SEGURIDAD DIGITAL

Identificación del riesgo

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información de los procesos de la Entidad.

Así mismo, es importante verificar posibles hechos que afecten la disponibilidad, integridad o confidencialidad de la información, a nivel físico o lógico, hardware, software y a nivel de instalaciones locativas o legales que lleven a afectar la información de la entidad o la privacidad de la información de una parte interesada e Incluye aspectos relacionados con el ambiente físico, digital y las personas, para lo cual se deben identificar los riesgos que afecten o vulneren las siguientes propiedades de la información:

Tabla 11 Propiedades de la información

Propiedades de la información	Descripción
Confidencialidad	Propiedad de la información que la hace no disponible; es decir, que no puede ser divulgada a individuos, entidades o procesos no autorizados.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Integridad	Propiedad de exactitud y completitud.

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

Las amenazas son de origen natural o humano y pueden ser accidentales o deliberadas, algunas amenazas pueden afectar a más de un activo generando diferentes impactos. Algunas de las amenazas consideradas en la norma ISO 27005:2008 son: Virus informático y software malicioso, avería de origen físico, errores de monitorización (log's), errores de usuarios, corte de suministro eléctrico, fallas eléctricas, daños por agua, fallo de comunicaciones, degradación de los soportes principales de almacenamiento de información, fenómeno natural, derrame de líquidos o sólidos, fuego, entre otras.

Para llevar a cabo este proceso se recomienda dar respuesta a los siguientes interrogantes:

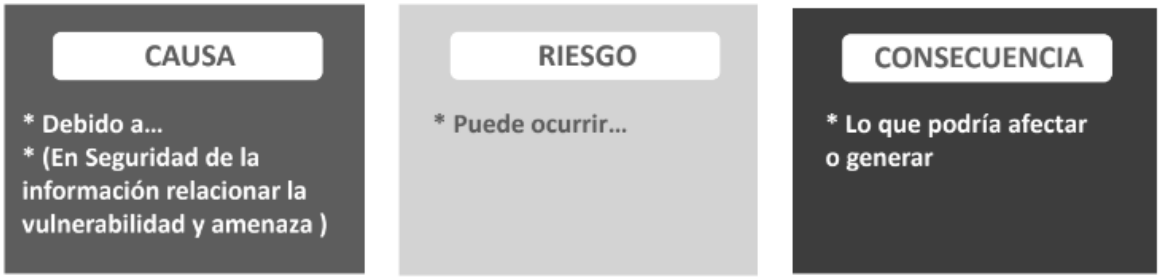


Ilustración 15 Redacción de riesgo de seguridad de la informaciónFuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

1.10.4 RIESGO FISCAL[2]

Identificación del riesgo

La estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos10 Concepto CGR-OJ-115 -2021 de la Contraloría General de la República, ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, se define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

¿Qué?	¿Cómo?	¿Por qué?
Impacto – Efecto Dañoso	**Circunstancia Inmediata**	**Causa Raíz-Potencial Hecho Generador**

[2] Tomado de " *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6* "

Posibilidad de efectos dañoso sobre <u>bienes públicos</u>	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

✓ **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).

✓ **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

Nota: *El análisis y la valoración continúa siguiendo la metodología establecida para la Guía de Administración del riesgo del Departamento Administrativo de la Función pública- DAFP*

<u>Revisión y evaluación</u>

La evaluación y revisión del riesgo es responsabilidad de la primera línea de defensa, la cual debe:

- Garantizar que los controles son eficaces tanto en el diseño como en la operación.
- Obtener información adicional para valorar el riesgo.
- Analizar y aprender lecciones.
- Verificar, atender e informar la materialización del riesgo.

Como parte del seguimiento a los controles, la primera línea de defensa reportará a la segunda línea de defensa cuatrimestralmente las actividades de control desarrolladas, junto con las evidencias soporte.

Con respecto a los cambios en el contexto estratégico del Instituto o a los cambios en la ejecución de los procesos o procedimientos, estos se deben revisar y actualizar en el mapa de riesgos de gestión, corrupción y seguridad de la información, de lo contrario se verificará que ningún hecho afecte la operación del Instituto.

Un aspecto fundamental para la administración del riesgo son las capacitaciones, las cuales se realizarán una vez al año (interna o externamente), de tal manera que permitan fortalecer las competencias de los servidores públicos, y así garantizar una gestión del riesgo coherente y adecuada dentro de los procesos.

1.11 Monitoreo

La gestión del riesgo se constituye como una herramienta para el cumplimiento de los objetivos de los procesos y de la entidad. A partir del Modelo Integrado de Planeación y Gestión - MIPG, mediante la incorporación de las líneas de defensa como esquema de control que define los roles y responsabilidades de todos los actores involucrados.

Para tal fin, y de acuerdo con la cultura del autocontrol cada responsable de proceso debe realizar el respectivo monitoreo a los riesgos de gestión, de corrupción y de seguridad de la información, en la herramienta dispuesta por la Oficina Asesora de Planeación. Igualmente, se debe realizar el respectivo seguimiento a la aplicación del tratamiento del riesgo establecido.

Además, los responsables de los procesos junto con su equipo realizarán mínimo anualmente la elaboración y/o actualización del mapa de riesgos (gestión, de corrupción, fiscal y/o seguridad de la información), sin embargo, dependiendo de las dinámicas propias de los procesos, los cambios en el contexto pueden presentarse en cualquier momento, por lo que de ser necesario se realizará actualización de la matriz cuando, así lo considere pertinente el líder del proceso en cualquiera de sus componentes (riesgos, controles, valoración) y son ellos quienes realizarán el monitoreo y la evaluación permanente al mismo, en los plazos establecidos.

La periodicidad del seguimiento realizado por los líderes de los procesos debe ser obligatoria y deben entregarse los resultados según requerimientos de la Oficina de Control Interno y/o la Oficina Asesora de Planeación, los cuales se establecen en la siguiente tabla:

Tabla 12 Seguimiento al mapa de riesgos y controles

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	ESTRATEGIA DE TRATAMIENTO - CONTROLES
RIESGOS DE GESTIÓN, SEGURIDAD DIGITAL y FISCALES	Baja	Se realiza seguimiento a los controles con periodicidad cada CUATRIMESTRAL (CUATRO MESES)
	Moderada	Se realiza seguimiento a los controles con periodicidad BIMENSUAL
	Alta	Se realiza seguimiento a los controles con periodicidad MENSUAL
	Extrema	Se realiza seguimiento a los controles con periodicidad MENSUAL
RIESGOS DE CORRUPCIÓN	Todos los riesgos de corrupción serán monitoreados de acuerdo a la zona del riesgo en la que se encuentran para el caso de MODERADO de manera TRIMESTRAL, y en zona ALTA Y EXTREMA de manera MENSUAL	

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

La Oficina Asesora de Planeación, tiene la responsabilidad de asesorar y guiar a la línea estratégica y la primera línea de defensa, en la gestión adecuada de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales y de los procesos, revisará que se cumpla con la presente metodología y liderará la consolidación de la información y su publicación. Para lo cual, publicará el mapa de riesgos de corrupción anualmente antes del 31 de enero de cada año y realizará el monitoreo cuatrimestral a la gestión del riesgo.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del mapa de riesgos de corrupción en la página web de la entidad.

- Hacer seguimiento a la gestión del riesgo.
- Revisar los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.
- Generar un informe sobre el resultado del monitoreo a los riesgos.

1.12 Seguimiento de riesgos

La Oficina de Control Interno realiza el seguimiento de manera independiente y objetiva al cumplimiento tanto de los objetivos institucionales como de los procesos. Asimismo, entrega su informe, de acuerdo con el programa de auditorías, al Comité Institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno. A la par, cuatrimestralmente realiza seguimiento a la gestión del riesgo, basándose en la revisión y resultados del monitoreo a los riesgos identificados y gestionados de la entidad. Las fechas de seguimiento serán las adaptadas por el IDEAM para cumplir con las definidas a continuación:

Tabla 13 Fechas de seguimiento a riesgos de la entidad

Seguimiento	Fecha	Publicación
1.er seguimiento	Corte al 30 de abril	Dentro de los diez (10) primeros días del mes de mayo.
2.o seguimiento	Corte al 31 de agosto	Dentro de los diez (10) primeros días del mes de septiembre.
3.er seguimiento	Corte al 31 de diciembre	Dentro de los diez (10) primeros días del mes de enero.

Fuente: *Guía para la gestión del riesgo de corrupción, 2015*.

1.13 Materialización del riesgo

En caso de materialización del riesgo, las acciones para seguir irán encaminadas hacia el análisis de causas y ajustes necesarios a la matriz de riesgos. De igual manera se tomarán las siguientes medidas:

Riesgo de corrupción: Informar a las autoridades de la ocurrencia de este hecho; revisar el mapa de riesgos, en particular las causas y los controles; y, realizar un monitoreo permanente para evitar la recurrencia.

Riesgo de gestión, seguridad digital y fiscales: Hacer una descripción detallada de lo ocurrido y del impacto generado en el proceso; revisar las causas y los controles. Realizar el análisis del riesgo teniendo en cuenta que varía la probabilidad; redefinir acciones que eviten la materialización del riesgo y actualizar el mapa de riesgos; y, realizar un monitoreo permanente.

La materialización del riesgo se deberá reportar a la segunda línea de defensa, que a su vez hará lo propio al Comité Institucional de Coordinación de Control Interno, en caso de que la materialización del riesgo haya afectado el cumplimiento de objetivos de la entidad.

En el evento de materializarse un riesgo de corrupción es necesario realizar los ajustes necesarios con acciones, tales como:

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4) Realizar un monitoreo permanente.

Para los riesgos de corrupción, su materialización puede derivar en acciones legales y pérdida de imagen para el instituto, estas acciones disciplinarias no solo caerán en las personas implicadas, sino también en los líderes de los procesos.

1.14 Actualización a la matriz de riesgo

Cuando el equipo responsable del proceso, producto del seguimiento y la revisión quisiera ajustar la redacción de un riesgo, incluir o eliminar algún riesgo identificado al inicio de la vigencia, el responsable del proceso deberá remitir un correo electrónico al jefe de la Oficina Asesora de Planeación con copia al profesional asignado, en el que se indique la justificación por la cual requiere que se realice la inclusión, modificación o eliminación del riesgo. La Oficina Asesora de Planeación realizará el análisis de esa información y generará sus observaciones, las cuales pueden ser aprobadas o no, dependiendo de la justificación aportada. Si los ajustes proceden dará respuesta favorable al proceso vía correo electrónico y se ajustará la matriz de riesgos institucional.

En caso de que sea eliminado un riesgo no se remueve de la matriz de riesgos, este quedará en estado finalizado, manteniendo el número consecutivo asignado, de tal manera que el riesgo mantenga su codificación y se pueda llevar trazabilidad de este.

1.15 Comunicación y consulta

El consolidado de los mapas de riesgo se publicará en la página web de la entidad, *link* de transparencia, numeral 6.4 "Planeación".

Se deberá realizar la socialización del mapa de riesgos de corrupción de la entidad a servidores públicos, contratistas y ciudadanía en general, de forma previa a su publicación, con el fin de recibir observaciones para su mejora.

Es responsabilidad de los líderes de proceso la socialización de los resultados obtenidos entre los miembros de su equipo y es responsabilidad de cada servidor consultar permanentemente los riesgos documentados a fin de tener reconocimiento de las situaciones de riesgo existentes y de las nuevas condiciones.

Este documento fue aprobado en sesión del 11 de julio de 2023, del Comité Institucional de Gestión y Desempeño

2. Documentos relacionados

República de Colombia. Departamento Administrativo de la Función Pública. (2022). *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6*. Bogotá: Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional.

3. Bibliografía

República de Colombia. Departamento Administrativo de la Función Pública. (2022). *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6*. Bogotá. Departamento Administrativo de la Función Pública, Dirección de Gestión y Desempeño Institucional.

4. CONTROL DE CAMBIOS

Versión	Fecha	Descripción
001	27/08/2019	Creación del documento.
002	19/03/2021	Actualización de la política de administración del riesgo y guía incluyendo los criterios de la guía del DAFP.
003	30/06/2021	Actualización del alcance en el cual se incluyen operaciones estadísticas De igual manera, se actualizan el marco normativo y los roles de las líneas de defensa de acuerdo con el Manual de MIPG, 2021.
004	25/01/2022	La actualización a la política de riesgos obedeció a la necesidad de mencionar la integralidad de los riesgos institucionales, resaltar la obligatoriedad de todas las áreas y colaboradores, involucrar el "MIPG"; resaltar el enfoque estratégico de los mismos, y adoptar expresamente la guía para la administración de riesgos y diseño de controles versión 5
005	11/07/2023	Actualización a la política de riesgos, actualización de metodología, inclusión de riesgos fiscales y seguridad e la información diseño de controles de acuerdo a la metodología del DAFP