IDEAM

SGI-PL019

POLÍTICA DE **ADMINISTRACIÓN DEL RIESGO**

2025

Introducción

La gestión del riesgo se constituye en un componente esencial para el fortalecimiento institucional y la garantía del cumplimiento misional del Instituto de Hidrología, Meteorología y Estudios Ambientales (Ideam). A través de un enfoque preventivo y sistemático, la gestión del riesgo permite identificar, analizar y mitigar eventos que puedan generar desviaciones en el logro de la misión, visión, objetivos estratégicos y operativos del Instituto, contribuyendo así a una administración pública más eficiente, transparente y orientada a resultados.

En este sentido, el Ideam ha adoptado un enfoque estructurado para la administración del riesgo, fundamentado en los lineamientos establecidos en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas", emitida por el Departamento Administrativo de la Función Pública (DAFP) y el "anexo 4 del Modelo de Gestión de Riesgos de Seguridad Digital" de MINTIC". Estos documentos proporcionan un marco metodológico que facilita la identificación de eventos de riesgo, la valoración de su impacto y probabilidad, así como la definición e implementación de controles eficaces que minimicen su ocurrencia o mitiguen sus efectos. Como insumo, para la identificación de riesgos y oportunidades organizacionales, se debe establecer el contexto y posteriormente identificar los riesgos y oportunidades por cada uno de los procesos. . Así mismo, cuando se materializa un riesgo de seguridad digital, se debe activar el procedimiento de gestión de incidentes y notificar a las entidades competentes. Por otro lado, se responden a los lineamientos emitidos por Superintendencia Financiera de Colombia en cuanto a gestión para identificar, evaluar y controlar los riesgos de lavado de activos y financiación del terrorismo a través de SARLAFT

La implementación de esta política de gestión del riesgo no solo responde a un mandato normativo, sino que se alinea con las buenas prácticas de gobernanza institucional. A través del fortalecimiento de sus capacidades internas para anticiparse y responder proactivamente a las amenazas. El Ideam avanza hacia una cultura organizacional más resiliente, capaz de adaptarse a los cambios del entorno y asegurar la sostenibilidad de sus procesos.

Objetivo

Gestionar los riesgos que puedan afectar la operación y cumplimiento de objetivos de acuerdo con el marco normativo vigente.

Objetivos específicos

- Mantener los riesgos institucionales en niveles bajos o moderados con controles con enfoque preventivo.
- Involucrar y comprometer a todos los servidores de las entidades de la Administración Pública en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.

- Mejorar el desempeño de la gestión del riesgo contribuyendo al logro de los objetivos a través de la identificación y tratamiento de eventos de materialización.

Alcance

Aplica a todos los procesos definidos en el Modelo de Gestión por Procesos, así como a las actividades desarrolladas por los servidores públicos en la sede central, sede de puente Aranda, aeropuertos, estaciones y áreas operativas del Instituto. Su propósito es establecer un marco integral que permita identificar, analizar, valorar, tratar y monitorear los riesgos de gestión, corrupción, fiscales, lavado de activos, financiación del terrorismo y de seguridad de la información, bajo el enfoque de las tres líneas de defensa. La primera línea, conformada por los líderes de proceso y responsables operativos, es la encargada de gestionar directamente los riesgos; la segunda línea realiza el seguimiento y acompañamiento técnico a la gestión del riesgo; y la tercera línea, a través de la Oficina de Control Interno, efectúa evaluaciones independientes que fortalecen la mejora continua del sistema.

Para la gestión de riesgos de seguridad de la información se debe considerar el MSPI conforme a los activos de información, la efectividad de los controles, la documentación e indicadores relacionados con el enfoque global de la organización hacia la gestión del riesgo.

Definiciones[1]

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.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

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.

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.

[1] Todo lo desarrollado en este numeral es tomado de " *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas versión 6* "

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.

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

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. 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 Integridad: Propiedad de exactitud y completitud.

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.

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

Evento De Materialización De Riesgo: el cual se define como una fuente de materialización del riesgo, un incidente que puede producir la materialización del riesgo.

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 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)" . 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". 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.

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.

Materialización De Riesgo: es la ocurrencia del riesgo, es decir, se convierte en una realidad y genera un impacto tangible.

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.

Monitoreo de riesgo: es la actividad que se realiza a fin de garantizar que las condiciones del riesgo no han cambiado y que no se está superando los niveles de tolerancia establecidos,

Su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como evaluaciones periódicas (autoevaluación, auditorías) que permiten valorar: (i) la efectividad del control

interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública

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.

Oportunidades: efectos 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.

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).

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.

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.

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, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

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

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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

Riesgo de Lavado de Activos /Financiación del Terrorismo: Posibilidad de pérdida o daño que podría sufrir la entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas.

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

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

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

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

Tratamiento de riesgo: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, los cuales estarán enfocados en aceptar, reducir, evitar y/o compartir el riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Siglas

MIPG: Modelo Integrado de Planeación y Gestión
DAFP: Departamento Administrativo de la Función Pública
TICs: Gestión de las Tecnología de la Información y la Comunicaciones
MECI: Modelo Estándar de Control Interno
LAFT: Lavado de Activos, Financiación del Terrorismo
MSPI: Modelo de seguridad y privacidad de la información

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.** En el que se define los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Así como define que 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.
- **Resolución 500 de 2021.** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- **Resolución 746 de 2022.** Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021

- **CIRCULAR EXTERNA PRESIDENCIA DE LA REPUBLICA 001 DE 2022.** Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.
- **NTCPE 1000-2020.** Norma Técnica de la Calidad del Proceso Estadístico. Requisitos de Calidad para la Generación de estadísticas. DANE-ICONTEC.
- **NTC ISO 27005:2009.** Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo en la Seguridad de la Información
- **NTC ISO 31000:2018.** Gestión del Riesgo – Principios y Directrices. Política de administración del riesgo.
- **Circular No. 100-000016 del 17 de noviembre de 2021**, emitido por Superintendencia de Sociedades; el cual indica que el rol del oficial de cumplimiento es el de participar activamente en los procedimientos de diseño, implementación, auditoría, verificación de cumplimiento y monitoreo del El Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos y Financiación del Terrorismo –SAGRILAFT.
- **Circular externa No. CIR25-00000026 / GFPU 13130000 de 6 de junio de 2025,** emitida por la Presidencia de la República, a través de la Secretaria de Transparencia; la cual establece lineamientos en maro del régimen de transición a los programas de transparencia y ética pública
- **Anexo 4 Modelo de Gestión de Riesgos de Seguridad Digital de MinTIC**: Marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta al momento de llevar a cabo actividades socio económicas en el entorno digital.

Promesa de Valor en la Gestión 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 con enfoque preventivo, participativo y orientado a resultados, promoviendo la capacidad e integridad de su talento humano como factor determinante para el aseguramiento de la transparencia y la confianza pública. Su ciclo de gestión se estructura en torno al análisis del contexto, identificación, valoración, monitoreo, tratamiento, revisión y evaluación de los riesgos que puedan afectar los objetivos organizacionales. Esta política se aplica de manera transversal a todos los niveles, procesos y áreas del Ideam, garantizando una respuesta coordinada y eficaz ante posibles amenazas que impacten su misión y buscando la mejora continua en gestión.

La Política de Administración de Riesgos se adopta, incluyendo aspectos relacionados con la adecuada administración del riesgo, según el Modelo Integrado de Planeación y Gestión – MIPG. Esta política se construye desde el direccionamiento estratégico y planeación con el fin de establecer los lineamientos para el tratamiento, manejo, prevención y seguimiento a los riesgos que pueden llegar a afectan los objetivos institucionales.

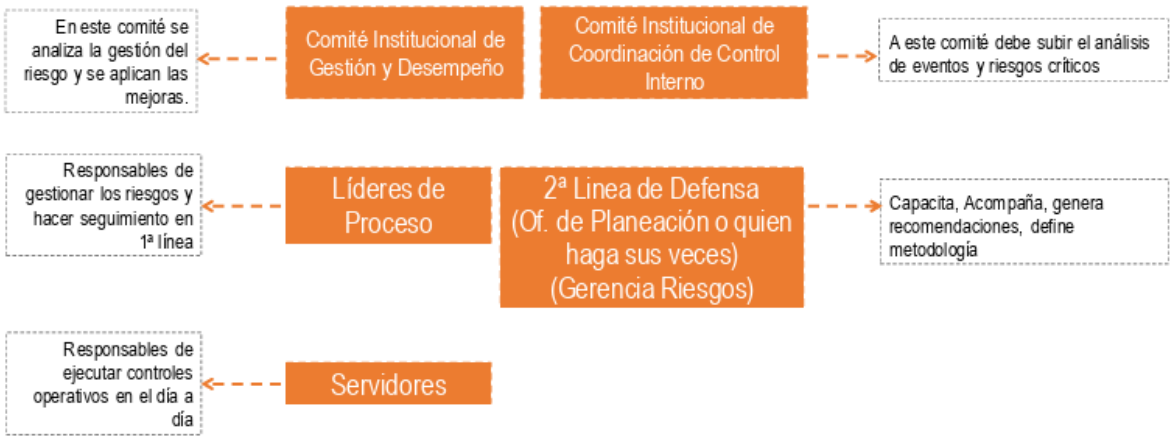
El Ideam entiende la importancia de la gestión de los riesgos de corrupción, de gestión, fiscales, de lavado de activos y financiación del terrorismo y de seguridad de la información (para activos con nivel crítico alto), en donde dispone de un equipo profesional especializado y de tres líneas de defensa y una línea estratégica para realizar un seguimiento detallado y evitar una posible materialización de algún riesgo que genere repercusiones en la entidad.

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.

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, asegurando los niveles de coordinación y comunicación en las diferentes etapas de esta gestión, de acuerdo con la siguiente estructura definida por la DAFP:

Ilustración 1 Niveles de coordinación y comunicación en las diferentes etapas de la gestión del riesgo



Fuente: Guía de administración del riesgo DAFP 2022

Por lo que se describen los roles y responsabilidades de la siguiente manera:

Tabla 1 Roles y responsabilidades de las líneas de defensa respecto a la gestión del riesgo

Línea de defensa	**Conformada por**	**Funciones frente a la gestión del riesgo**
Línea de defensa estratégica	Dirección general, Comité Institucional de Control Interno	✓ Emitir, revisar, validar y supervisar políticas de la entidad en materia de administración de todos los riesgos que pueden afectar los objetivos de la entidad. ✓ 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). ✓ Definir el marco general para la gestión del riesgo y el control, proveer los recursos necesarios para su implementación, garantizar el cumplimiento de los planes de la entidad y asegurar la mejora continua de la gestión y el desempeño de la entidad
Primera línea de defensa	Servidores en sus diferentes niveles, líderes o	✓ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar

	responsables de proceso	los que ya se tienen identificados en cada uno de sus procesos, y así realizar la actualización respectiva de la matriz de riesgos de cuando se requiera. (contexto estratégico, identificación y valoración de riesgos). ✓ Mantener controles internos efectivos; por consiguiente, identificar, evaluar, controlar y mitigar los riesgos. Aspectos que debe tener en cuenta la línea de defensa: ✓ Promover 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. ✓ Identificar los riesgos y el establecimiento de controles, así como el seguimiento, acorde con su diseño, con el fin de evitar la materialización de estos, en los tiempos establecidos. ✓ 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, talento humano y de	✓ Acompañar y orientar a los líderes de procesos, en la gestión integral del riesgo lo que comprende las fases de identificación, análisis y valoración, monitoreo y tratamiento de los riesgos identificados ✓ Revisar el adecuado diseño de los controles para la mitigación de los

	Oficina de Informática	riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. ✓ Liderar el proceso de construcción del mapa de riesgos de acuerdo con la tipología descrita en esta política. ✓ Apoyar a la Alta Dirección y a los líderes de proceso para un adecuado y efectivo ejercicio de la gestión de los riesgos que afectan el cumplimiento de los Objetivos Estratégicos de la Entidad. ✓ Informar sobre la incidencia de los riesgos de los activos de información en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada. ✓ Seguir los resultados de los planes de tratamiento desarrollados e implementados para mitigar los riesgos sobre los activos de información cuando haya lugar. ✓ Analizar y consolidar los seguimientos y las actualizaciones realizadas en el mapa de riesgos. ✓ 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. ✓ 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 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 a los responsables y ejecutores de los procesos y proyectos (primera línea) como complemento a la labor de acompañamiento que desarrollan la Oficina Asesora de Planeación y el Comité Institucional de Gestión y Desempeño 8segunda línea de defensa), 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. ✓ A través de procesos de asesoría y/o consultoría 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. ✓ Fortalecer la gestión del riesgo institucional con la identificación de señales de alerta (riesgos emergentes) en los ejercicios de auditoría interna, para garantizar la integridad y eficacia de los procesos internos

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

Estrategias para la administración del riesgo

Las estrategias que permiten alcanzar los objetivos de la entidad, por medio del buen manejo de la administración de los riesgos requiere:

- Acciones de autocontrol en los equipos de trabajo frente a objetivos, metas, indicadores, riesgos, etc. (primera línea),
- Ejercicios de autoevaluación que faciliten el aseguramiento de la gestión y la toma de decisiones para el mejoramiento del control interno y la gestión de riesgos (segunda línea).
- Fortalecimiento de la cultura del riesgo a través de la capacitación, sensibilización y conocimiento de los lineamientos y metodología de gestión integral de riesgos del instituto
- Evaluar la gestión de riesgos y revisar los factores críticos desde la alta dirección.

I. Metodología para la administración del riesgo

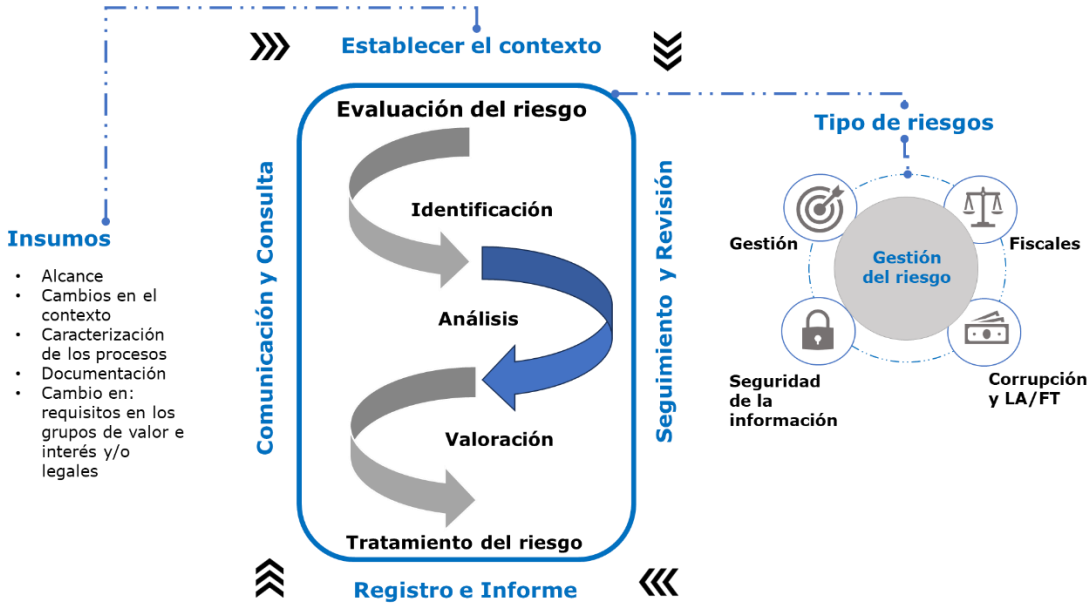
El Ideam como Entidad pública ha estructurado la metodología para el desarrollo y cumplimiento de su Política Integral para la Administración del Riesgo a partir de los lineamientos que en esta materia ha impartido el Departamento Administrativo de la Función Pública mediante la Guía para la administración del riesgo y el diseño de controles en entidades públicas en la versión vigente, en donde establece los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de gestión, corrupción, de seguridad de la información, fiscales y LA/FT. 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.

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

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

En ese sentido, es importante conocer y analizar los insumos necesarios para la adecuada ejecución del ciclo de la administración del riesgo, el cual se describe a continuación:

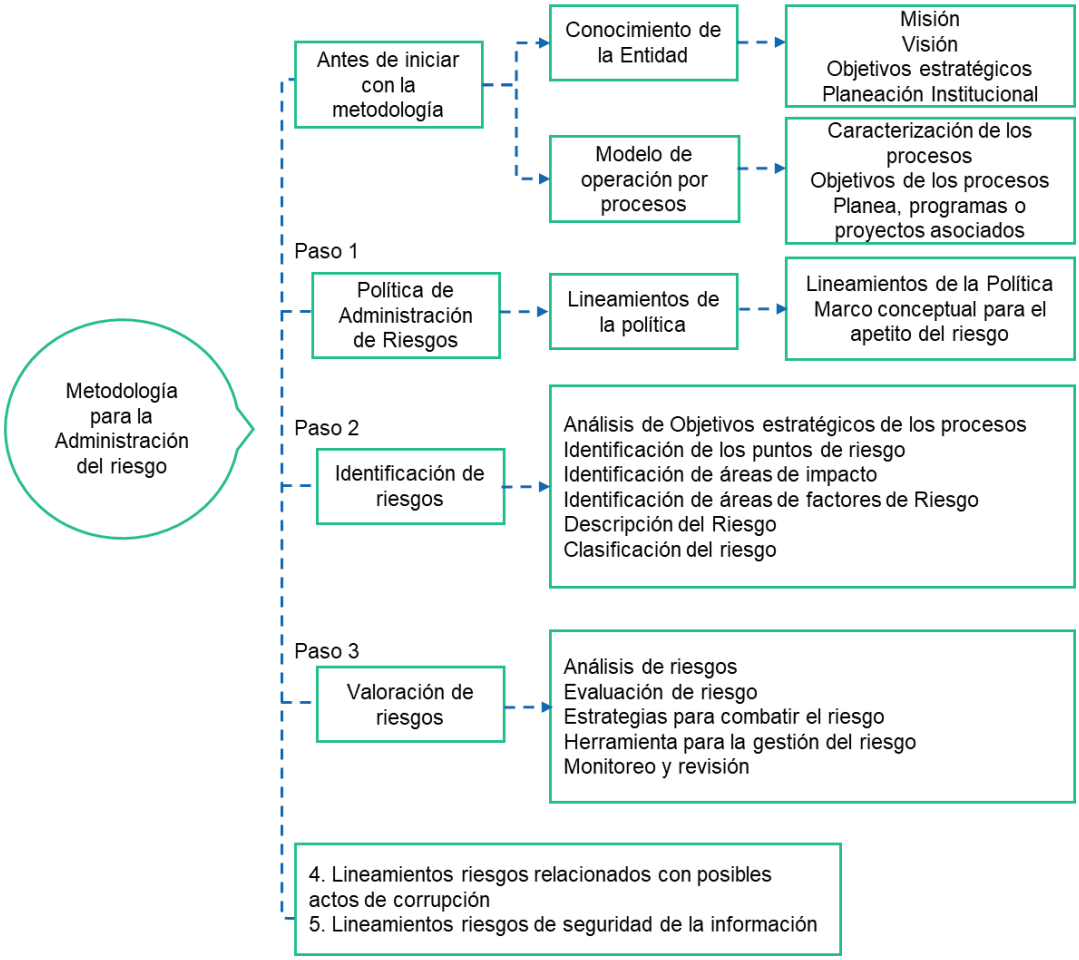
Ilustración 2 Ciclo de Gestión de la Administración del Riesgo



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

La estructura de la metodología aplicada para la administración de riesgos de gestión, corrupción, fiscales y SARLAFT se evidencia en la ilustración a continuación:

Ilustración 3 Metodología para aplicar correctamente la administración del riesgo



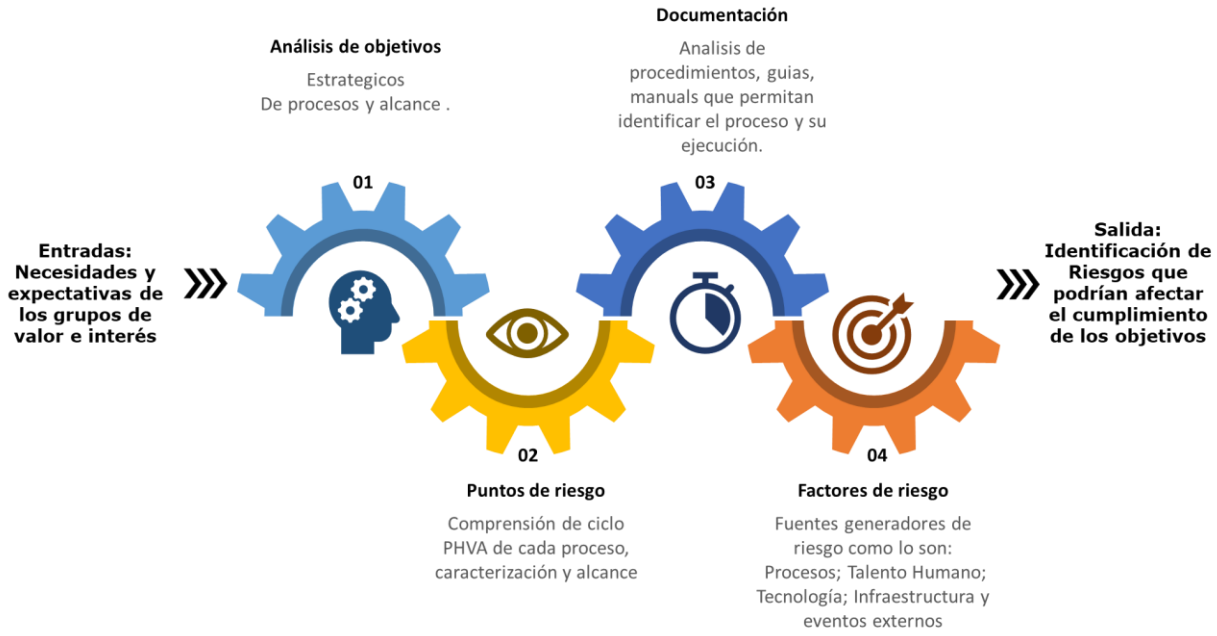
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas 2022

Ahora bien, con respecto a la metodología para la administración de riesgos de seguridad deben contemplarse las fases definidas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información vigente.

1. Identificación del riesgo

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos, por lo que se analizan los siguientes componentes:

Ilustración 4 Insumos para la identificación de riesgos



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

1.1 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.[2]

2. Tipología de riesgos

Una vez son analizados los diferentes factores, es necesario determinar la tipología del riesgo para así tener claridad para su correcta gestión, redacción y valoración, actualmente se cuenta con la siguiente clasificación:

Tabla 2 Tipo de riesgos

Tipo de riesgo	Descripción
Riesgos de Gestión	Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias. 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

[2] NTC ISO 31000, Numeral 2.9

	infraestructura o por la ocurrencia de acontecimientos externos. OOEE. Se asocian a los riesgos que se identifican en el cumplimiento e implementación de la NTCPE 1000: 2020 "Norma técnica de la calidad del proceso estadístico". Requisitos de calidad para la generación de estadísticas en el cual en su numeral ***4.7 Gestión de riesgos*** define que *"La entidad debe identificar y analizar los riesgos del proceso estadístico e implementar los controles para minimizarlos y tomar acciones cuando estos se materialicen."*[3], estos utilizan la misma metodología de los riesgos de gestión y corrupción de la Entidad.
Riesgos de Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. 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.
Riesgos Fiscales	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).
Riesgos 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 LA/FT	Posibilidad de pérdida o daño que podría sufrir la entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, se utilizará la metodología de riesgos de corrupción para su gestión.

[3] NORMA TÉCNICA DE LA CALIDAD DEL PROCESO ESTADÍSTICO, REQUISITOS DE CALIDAD PARA LA GENERACIÓN DE ESTADÍSTICAS - NTC PE 1000:2020

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

3. Descripción del riesgo

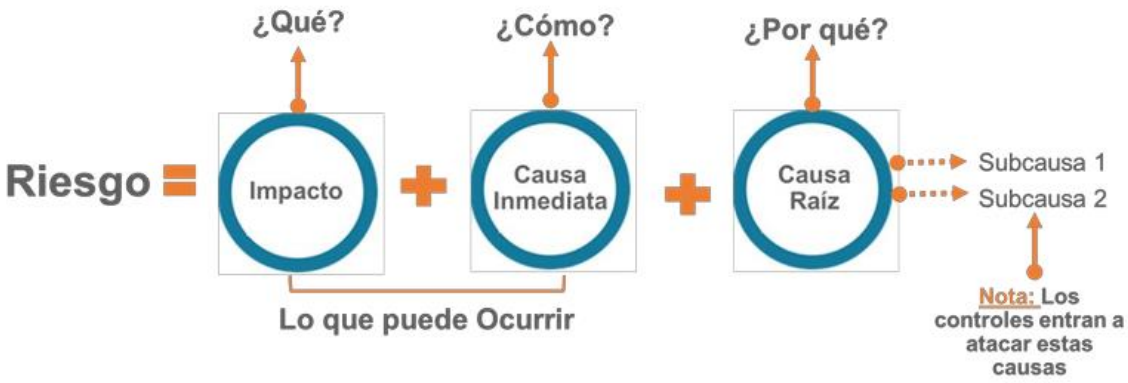
La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento, tanto para el líder del proceso como para personas ajenas al proceso.

Para cada tipología de riesgo se cuenta con una estructura en la redacción esto facilitará su identificación, por lo que a continuación, se detallaran:

3.1 Riesgo de Gestión

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 5 Redacción del riesgo de gestión



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.

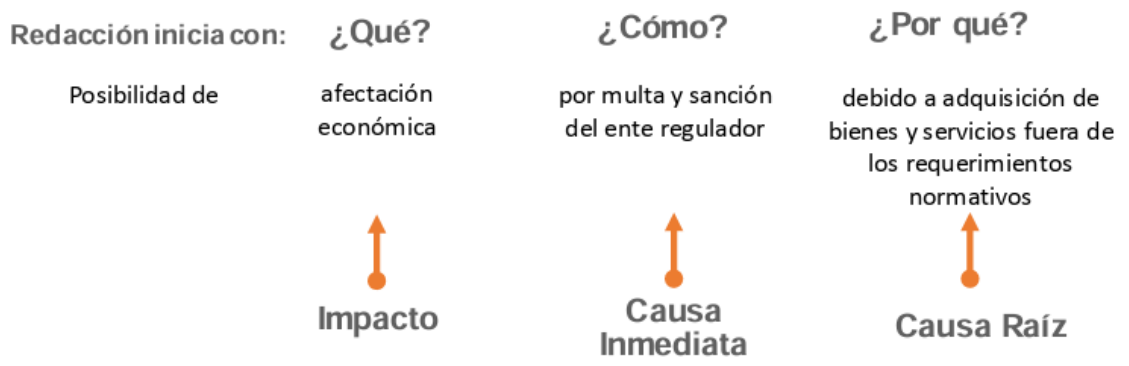
A continuación, se definen los elementos claves para la redacción del riesgo:

- 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 dañosa 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 6 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.

3.2 Riesgo de Corrupción

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, 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

Tabla 3 Matriz para la identificación de riesgos de corrupción.

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 un tercero con el fin de celebrar un contrato.	x	x	x	x

Fuente: Secretaría de Transparencia de la Presidencia de la República

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.

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.

3.3 Riesgo Fiscal

La estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; 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.

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 la estructuración del riesgo es importante tener en cuenta el impacto y la causa raíz, dado que, dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Y la causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

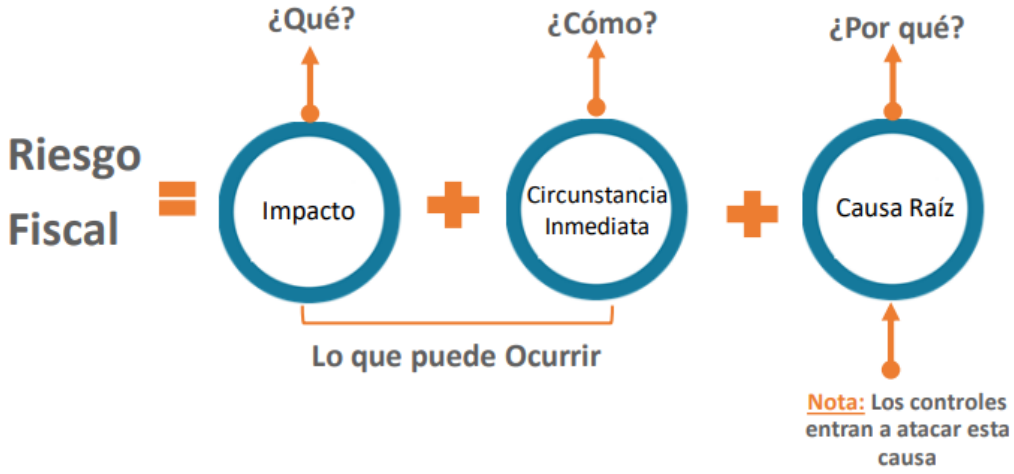
Por lo cual la estructura de la redacción de riesgos fiscales se conjugan los elementos descritos, y se debe tener en cuenta:

- Iniciar con la oración: *Posibilidad de*, debido a que nos estamos refiriendo al evento potencial.
- Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

- 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.[3]

De acuerdo con lo anterior, la estructura será así:

Ilustración 7 Estructura de riesgo fiscal



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

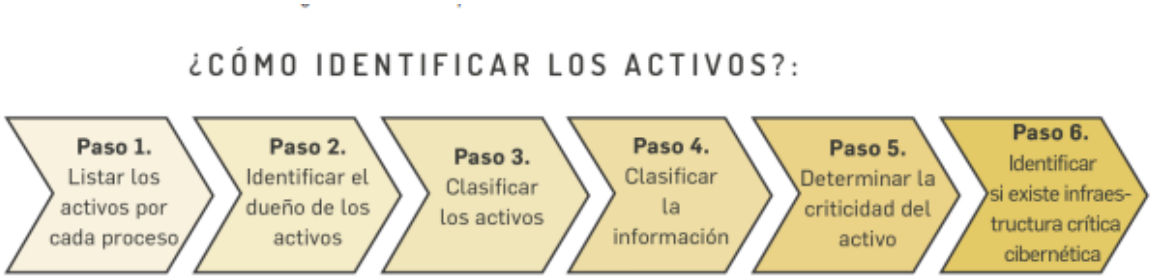
Para su análisis, valoración y materialización se deberá dar cumplimiento a la metodología descrita en la presente guía.

3.4 Riesgos de Seguridad de la Información

Se debe tener en cuenta el Modelo de Seguridad y Privacidad de la Información (MSPI) , el cual se encuentra alineado con el marco de referencia de arquitectura MRAE y soporta transversalmente los otros habilitadores de la política de gobierno digital.

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, por lo tanto, deben seguirse los siguientes pasos para establecer dichos activos:

Ilustración 8 Pasos para identificar activos de la información



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

El objetivo del enfoque preventivo para el riesgo de seguridad de la información y el cual debe primar en el Instituto, es buscar la mínima calificación del riesgo hasta que se logre llevarlo a un nivel Aceptable, y, por lo tanto, el riesgo que continúe con una valoración en zona de riesgo extrema, alta o moderada después de los controles.

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 4 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, 2022

Para la identificación del riesgo se podrán identificar los siguientes tres riesgos inherentes de seguridad de la información

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

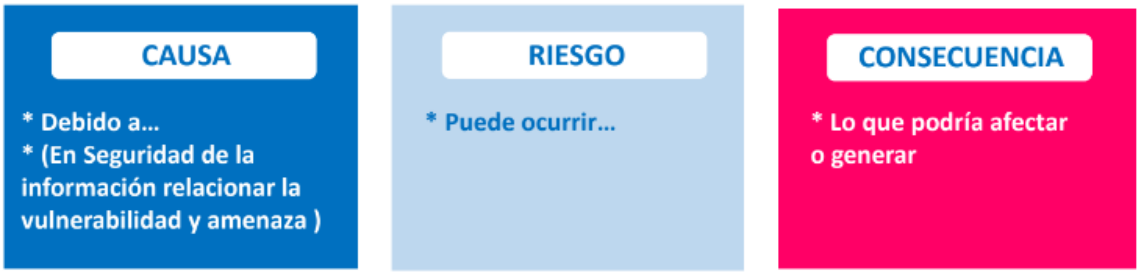
Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

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 27005:2009 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.

Es importante tener en cuenta los siguientes elementos para la redacción del riesgo de seguridad de la información:

Ilustración 9 Redacción de riesgo de seguridad de la información



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

Para la etapa de valoración de los riesgos se tomará como base lo definido en NTC ISO 27005:2009. Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo en la Seguridad de la Información y en NTC ISO 31000:2018. Gestión del Riesgo – Principios y Directrices.

3.5 Riesgos de lavado de activos y financiación del terrorismo

Con el fin de facilitar la identificación de riesgos de LA/FT, se debe verificar si cumple con la siguiente definición y posteriormente se debe analizar y calificar a partir de las consecuencias identificadas en la descripción del riesgo,

Posibilidad de pérdida o daño que podría sufrir la entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de

activos y/o canalización de recursos hacia la realización de actividades terroristas.

Se describen a continuación algunas señales de alerta que pueden ser orientadoras para la identificación de la posible materialización de estos riesgos:

A. Con los mecanismos y herramientas de verificación dispuestos durante la etapa precontractual por **la Oficina Asesora Jurídica:**

- Empresas inexistentes,
- Coincidencia en listas vinculantes y/o restrictivas
- Proveedores que constantemente trasladan su domicilio y/o cambian de razón social
- Tarifas ofrecidas por los proveedores con precios muy inferiores a los del mercado
- Presentación de documentos falsos, adulterados e ilegibles.
- Inconsistencias en la información relacionada con la existencia, identificación, dirección del domicilio, o ubicación de la parte relacionada.
- Tienen en común socios, gerentes, administradores o representantes legales con otras personas jurídicas o empresas investigadas por temas relacionados con LAFT.
- Cesión de los derechos de pago del servicio prestado a un tercero, sin que medie una reglamentación para ello

B. Con los mecanismos y herramientas de verificación dispuestos por **la Secretaria General, a través del grupo de Gestión del Desarrollo del Talento Humano:**

- Cesión de los derechos de pago del servicio prestado a un tercero, sin que medie una reglamentación para ello: en el trámite de nómina cuando el servidor remite su certificación bancaria se valida que sea a nombre propio.
- Presentación de documentos falsos, adulterados e ilegibles: desde vinculaciones, se hace validación de títulos y certificaciones laborales
- Tienen en común socios, gerentes, administradores o representantes legales con otras personas jurídicas o empresas investigadas por temas relacionados con LAFT: en la declaración de bienes y rentas se relaciona.

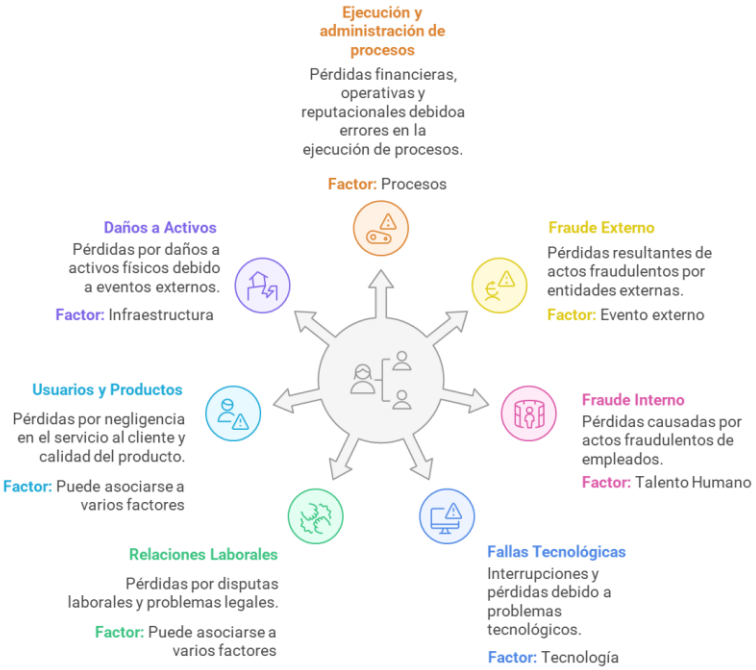
C. Con los mecanismos y herramientas de verificación dispuestos por **la Secretaria General, a través del grupo de Gestión Financiera:**

- Pago a personas distintas al beneficiario final, a solicitud del proveedor

4. 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:

Ilustración 10 Clasificación de factores de riesgos



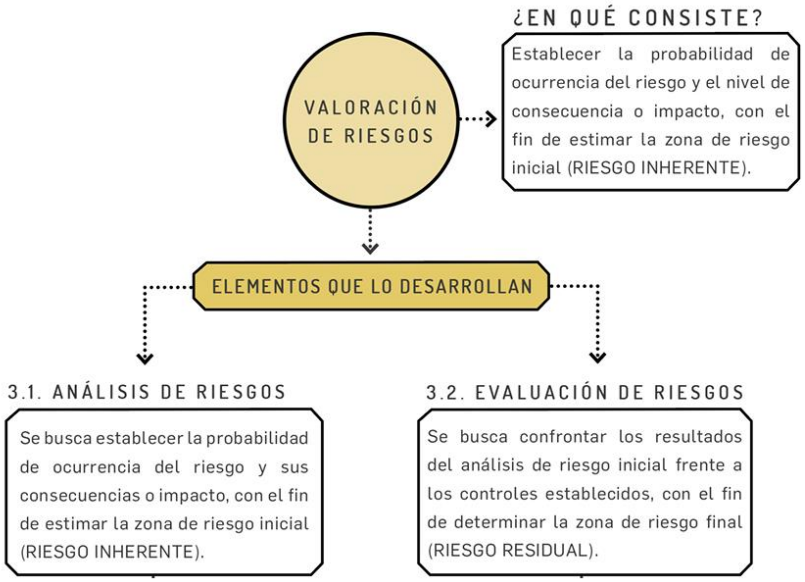
Fuente: Guía Para Para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2022.

5. Valoración del Riesgo

En este apartado, se pretende establecer la probabilidad de la ocurrencia del riesgo y el nivel de consecuencia o impacto, el cual permite estimar la zona de

riesgo inherente, desarrollando el análisis y evaluación de los riesgos que sean identificados por la Entidad, de acuerdo con la metodología y tipo de riesgo.

Ilustración 11 Valoración del riesgo



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

5.1 Riesgo de Gestión y Fiscales

Determinar la Probabilidad:

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

Tabla 5 Criterios 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 de funcionamiento = 1 vez Ej. Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60días *24 horas = 1440horas	Diaria	Muy Alta

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:

Ilustración 12 Criterios para definir la 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 2022

Determinar el Impacto:

Para la construcción de la siguiente 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.

Ilustración 13 Criterios para definir el impacto

	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

5.2 Riesgos de Corrupción y LA/FT

Determinación de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de **frecuencia o factibilidad**, donde **frecuencia** implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Tabla 6 Tabla de probabilidad para riesgos de corrupción

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años

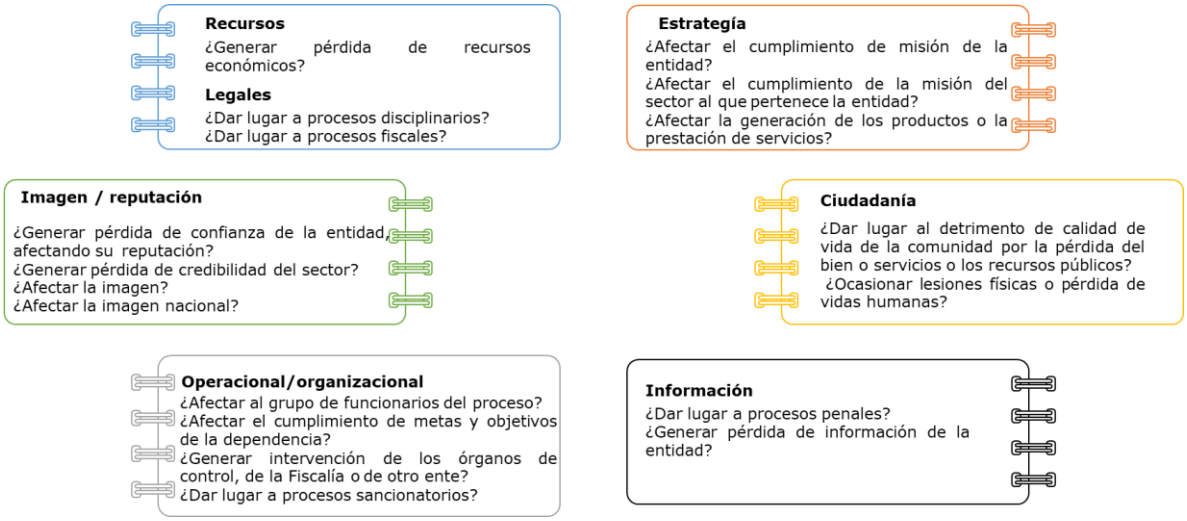
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes p anormales)	No se ha presentado en los últimos 5 años.

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

Determinación del impacto

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 7 Preguntas para determinar el impacto de riesgos de corrupción



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

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

Tabla 8 Definición del impacto en riesgos de corrupción por número de respuestas afirmativas

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, 2022

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

Para la definición de controles y monitoreo se debe implementar la misma metodología descrita en esta guía.

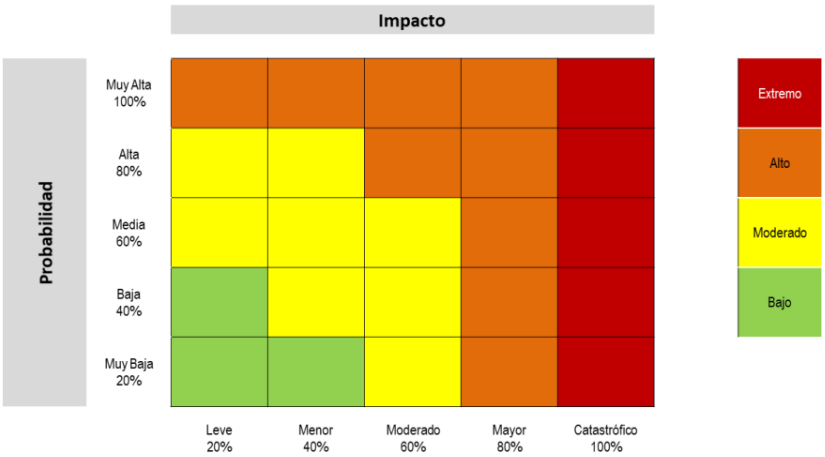
5.3 Evaluación de riesgo

A partir del análisis realizado de la probabilidad e impacto, se busca determinar la zona de riesgo inicial o Riesgo Inherente.

Por lo que se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Definiendo así 4 zonas de severidad en la matriz de calor.

La matriz de calor representa el nivel de severidad del riesgo, la cual se conforma por cinco (5) niveles de probabilidad y cinco (5) niveles de impacto, a excepción de los riesgos de corrupción cuyo nivel de impacto se mide en tres niveles: moderado, mayor y catastrófico, toda vez que no existe nivel de aceptación para este tipo de riesgos, y de los riesgos ambientales donde el nivel de impacto se mide en tres niveles: leve, moderado y catastrófico. Esta combinación de los dos factores de valoración en el riesgo representa cuatro (4) zonas de riesgo: Baja, media, alta y extrema.

Ilustración 14 Matriz de Calor (niveles de severidad del riesgo)



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

Ejemplo:

Proceso: Gestión de recursos

Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

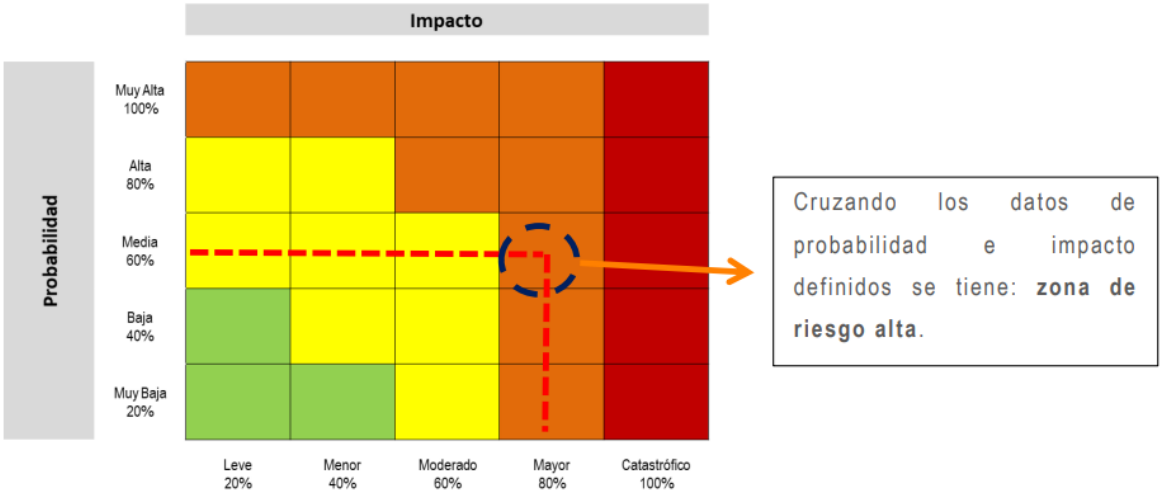
Riesgo identificado: Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

Probabilidad Inherente = Media 60%

Impacto Inherente: Mayor 80%

Aplicando el mapa de calor tenemos:

Ilustración 15 Ejemplo de cruce entre la probabilidad e impacto inherente en la matriz de calor



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

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 de acuerdo con la tipología y 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. En riesgos de corrupción no aplica el apetito ni la tolerancia al riesgo.

6. 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

Se propone una adecuada redacción del control así:

Responsable+ Acción+ Complemento

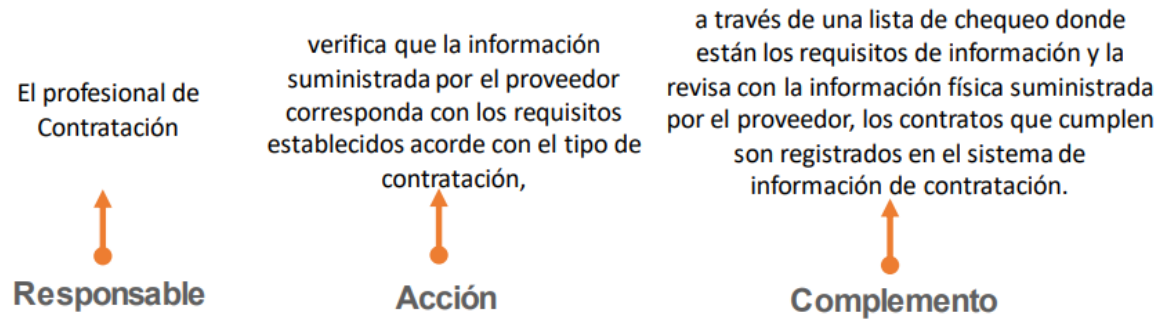
Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

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.

A continuación, se establece un ejemplo con la estructura:

Ilustración 16 Ejemplo de redacción de los controles con la estructura



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

NOTA: 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.

Por lo anterior deberá considerar dentro de las posibles desviaciones el flujo de ejecución del control teniendo en cuenta:

a) En caso de que el control haya sido efectivo, se notificará dentro del monitoreo realizado por la primera línea de defensa de acuerdo con lo establecido en las estrategias para la administración del riesgo
b) En caso de que el control no haya sido efectivo, dentro del seguimiento a los controles deberá ser descrito las acciones realizadas para asegurar el funcionamiento de los controles.

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:

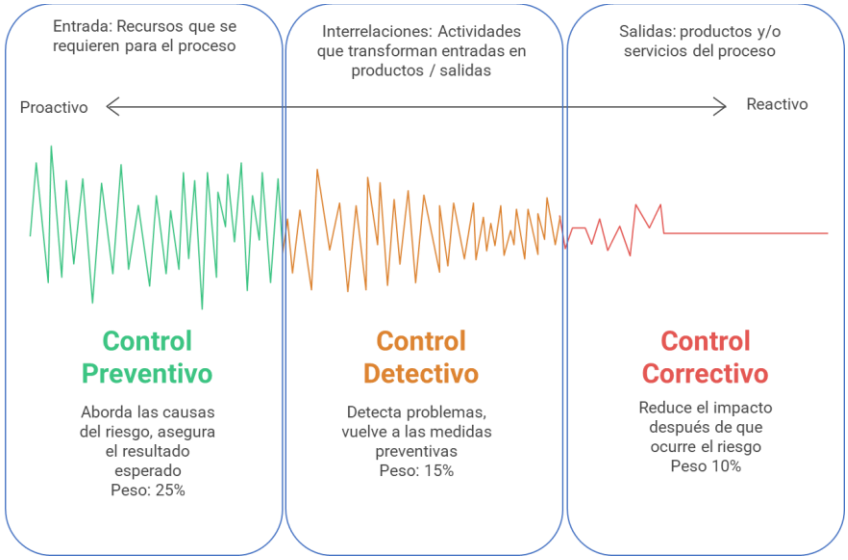
- Fue ejecutado por el responsable designado.
- Se realizó de acuerdo con la periodicidad establecida.
- Se cumplió con el propósito del control.
- Se evidencia tratamiento a las desviaciones detectadas durante la ejecución del control

7. Análisis y evaluación de los controles

7.1 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 y con ello su ponderación para la etapa de valoración de controles con mayor precisión. Para comprender esta estructura conceptual, en la siguiente ilustración se consideran 3 fases globales del ciclo de un proceso así:

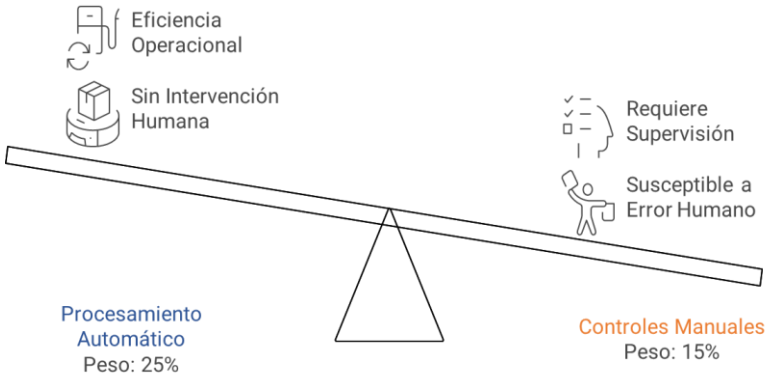
Ilustración 17 ciclo del proceso, las tipologías de controles y atributos de eficiencia



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

Adicionalmente se cuentan con los siguientes atributos y sus pesos:

Ilustración 18 Atributos de eficiencia por procesamiento automático y manual



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

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).

Ilustración 19 Atributos informativos de los controles de riesgos

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

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.

7.2 Controles asociados a la seguridad de la información

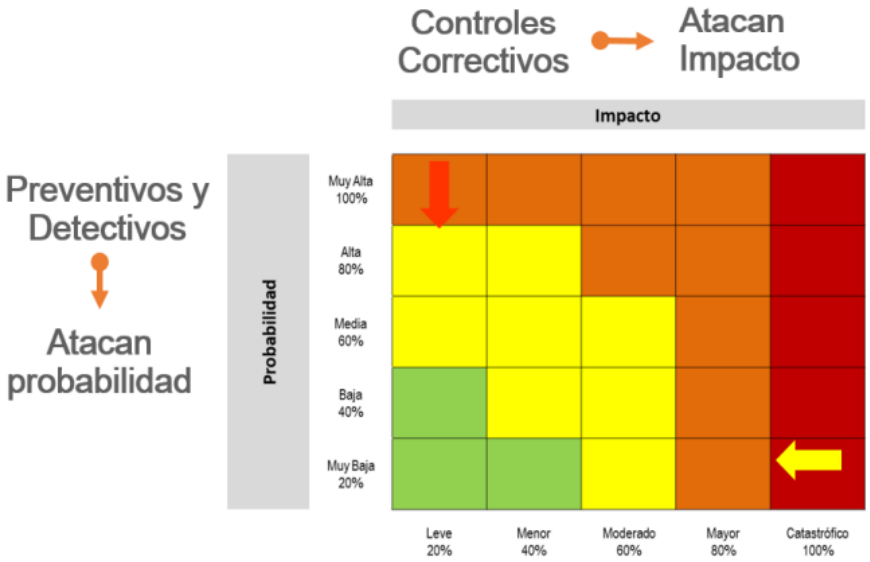
Los controles podrán elegirse los enlistados en la NTC ISO 27001 Tecnología de la Información, Técnicas de Seguridad Sistema de Gestión de la Seguridad en la Información – Requisitos anexo A.

Por lo que su valoración final serán parte de la metodología utilizada teniendo en cuenta las normas NTC:ISO nombradas anteriormente.

8. Nivel del riesgo (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, por lo que esto genera un desplazamiento en la matriz de calor, así:

Ilustración 20 Movimiento en la matriz de calor acorde con el tipo de control



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

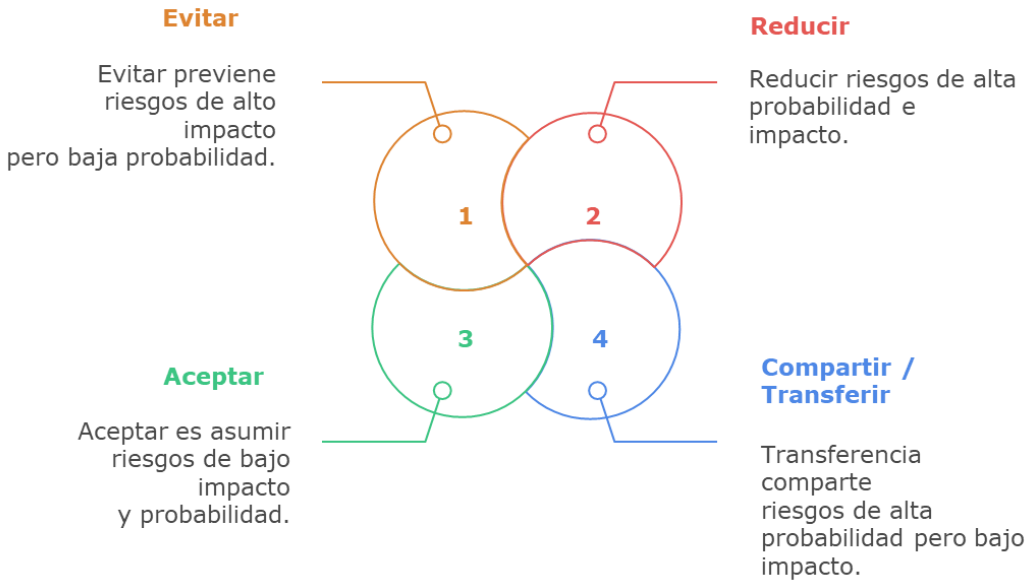
La evaluación del riesgo se realiza de acuerdo con los resultados que se obtengan en la matriz, teniendo en cuenta la valoración del riesgo residual:

- 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.

9. Estrategias para combatir el riesgo

Son las decisiones que se toman frente a un determinado nivel de riesgo en cual debe estar enfocada en aceptar, reducir, evitar o compartir / transferir, su análisis se genera a partir del riesgo residual para los procesos en funcionamiento, para el caso de los nuevos procesos esto se realizará a partir del análisis inherente.

Ilustración 21 Estrategias para combatir el riesgo



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

10. Tratamiento de riesgos en caso de materialización

Debido a la gestión del riesgo y su tratamiento es necesario recordar que existe:

1. Evento de materialización del riesgo
2. Materialización del riesgo

Cada uno de ellos requiere una gestión diferente:

En el caso de los eventos de materialización, estos deberán ser informados por cualquiera de las líneas de defensa a la oficina asesora de planeación mediante correo electrónico o el aplicativo o herramienta tecnológica definida desde la OAP para determinar estadísticas y/o la potencial identificación de acciones que a corto o mediano plazo pueda minimizar la ocurrencia o materialización de los riesgos.

En caso de materialización del riesgo, al igual que el evento de materialización deberá informarse a la Oficina Asesora de Planeación para que en conjunto con la primera línea se defina un análisis que permitan determinar la causa raíz de la ocurrencia y con ello establecer acciones que deberán irán encaminadas a la subsanación de la situación de modo en que se estructurarán y se llevarán a cabo actividades complementarias a los controles.

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, complemento y/o actualización de procedimientos, entre otras). La aplicación de nuevas acciones no sustituye la obligatoriedad de la aplicación de los controles estandarizados.

De igual manera se tomarán las siguientes medidas de acuerdo con el tipo de riesgo:

Riesgo de corrupción: En el caso 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, lo que puede desencadenar en acciones disciplinarias que aplicaran a quienes correspondan.

Riesgo de gestión 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 puede variar 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.

Para que un tratamiento sea válido **se debe demostrar con evidencia objetiva que el tratamiento planteado está siendo ejecutado**, por lo que se debe definir el **responsable** para cada tipo de actividad del plan de gestión de los riesgos, y explica sus responsabilidades y un **cronograma de implementación de acciones** en donde 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.

Riesgo de seguridad y privacidad de la información: la comunicación de la materialización de los riesgos debe estar articulada con la gestión de incidentes y el plan de recuperación de desastres. Así mismo, Las capacitaciones, entrenamientos, sensibilizaciones y piezas gráficas deben estar incluidas en el plan de uso y apropiación de seguridad.

11. Monitoreo

De acuerdo con la cultura del autocontrol cada responsable de proceso debe realizar el respectivo monitoreo a los riesgos de gestión, de corrupción y LA/FT, fiscales y de seguridad de la información, en la herramienta dispuesta por la Oficina Asesora de Planeación, en este caso en el aplicativo o herramienta tecnológica definido desde la OAP. 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 monitoreo realizado por la primera línea de defensa 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 tabla 9:

Tabla 9 Monitoreo de riesgo de acuerdo con su calificación residual

Tipo de Riesgo	**Zona de riesgo Residual**	**Estrategia de Tratamiento – Controles**
Riesgo de gestión, seguridad de la información y fiscales	Baja	Se realiza seguimiento a los controles con periodicidad cada CUATRIMESTRAL (CUATRO MESES)
	Moderada	Se realiza seguimiento a los controles con periodicidad BIMESTRAL
	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 BIMESTRAL, y en zona ALTA Y EXTREMA de manera MENSUAL	

Fuente: propia

En caso de que la primera línea de defensa no realice oportunamente el monitoreo y/o reporte de sus riesgos, la Oficina Asesora de Planeación emitirá alertas conforme al siguiente procedimiento:

1. Se enviará una primera alerta al líder del proceso mediante correo electrónico, informando la omisión detectada.
2. Si transcurridos 60 días desde la primera alerta no se ha realizado el monitoreo correspondiente, se remitirá un memorando formal en el que se indique la fecha en que debió haberse llevado a cabo dicha actividad.
3. Si después de 90 días persiste la falta de monitoreo, se enviará un nuevo memorando reiterando la situación, esta vez con copia a la Oficina de Control Interno Disciplinario para los fines pertinentes.

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 tanto de gestión como de corrupción anualmente antes del 31 de enero de cada año y realizará el seguimiento a la gestión del riesgo de la siguiente forma:

- Riesgos altos y extremos, seguimiento de segunda línea con corte del 01 de enero al 31 de marzo de la vigencia
- Riesgos Moderados, seguimiento de segunda línea con corte del 01 de abril al 30 de junio de la vigencia.
- Riesgos bajos, seguimiento de segunda línea con corte del 01 de julio al 30 de septiembre de la vigencia.
- Así mismo, durante toda la vigencia se realizará seguimiento a los eventos y materialización de riesgos reportados.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del mapa de riesgos identificados tanto de gestión como 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 anual.
- Revisión y Evaluación del riesgo
- 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 de acuerdo con la periodicidad

definida por la calificación residual 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, fiscal, corrupción, LA/FT 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.

La Oficina de Control Interno, en cumplimiento del Plan Anual de Auditorias aprobado para cada vigencia por parte del Comité Institucional de Coordinación de Control Interno, así como en su rol de tercera línea de defensa, llevará a cabo la revisión de los riesgos y controles de los procesos intervinientes en el marco del desarrollo de las Auditorias, Informes de Ley y Seguimientos a través de la plataforma aplicativo o herramienta tecnológica definido desde la OAP. Una vez se cuente con el informe final, se procederá a informar y retroalimentar a los procesos responsables y a la Oficina Asesora de Planeación para su correspondiente análisis.

12. 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 podrá informar (a) mediante correo electrónico a la Oficina Asesora de Planeación con copia al profesional asignado, (b) mediante mesa de trabajo con el encargado de la gestión de riesgos como segunda línea de defensa, o (c) mediante aplicativo o herramienta tecnológica definido desde la OAP, en la cual 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 inactivo, de tal manera que el riesgo mantenga su identificación y se pueda llevar trazabilidad de este.

II. Implementación

Para la implementación de la política de administración del riesgo, el Ideam definirá la herramienta tecnológica en la cual se realizará la identificación, análisis, valoración, monitoreo y tratamiento a los riesgos que sean identificados. 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. Operatividad en herramienta tecnológica

Para realizar la gestión del riesgo en el aplicativo, es fundamental iniciar con la identificación de roles y responsabilidades.

Este paso es clave, ya que permite establecer qué actores interactuarán con la gestión del riesgo dentro del sistema. La definición de los roles se realizará con base en las responsabilidades asignadas a cada usuario, de la siguiente manera:

Tabla 9 Roles y responsabilidades roles en herramienta tecnológica

Rol en el aplicativo o herramienta tecnológica definido desde la OAP	Responsabilidad
Administrador módulo de gestión de riesgos	Los usuarios adscritos a este rol tendrán la capacidad de realizar toda la gestión del riesgo (la identificación, valoración, monitoreo de los riesgos e identificación y seguimiento al tratamiento de los riesgos definidos por los líderes de los procesos).
Líderes de procesos	Los usuarios adscritos a este rol tendrán la capacidad de realizar el monitoreo y gestionar sus controles, entendiéndose como el cargue de las evidencias necesarias para soportar el monitoreo, el reporte de eventos de materialización y materialización de sus riesgos.
Gestores de cada uno de los procesos	Los usuarios adscritos a este rol tendrán la capacidad de realizar el monitoreo y gestionar sus controles, entendiéndose como el cargue de las evidencias necesarias para soportar el monitoreo, el reporte de eventos de materialización y materialización de sus riesgos.
Gestores de Segunda Línea de defensa	Los usuarios adscritos a este rol tendrán la capacidad de realizar el seguimiento de la primera línea de defensa, revisión de las evidencias

	aportadas y seguimiento a la materialización de riesgos
Gestores de Tercera Línea de defensa	Los usuarios adscritos a este rol tendrán la capacidad de realizar el seguimiento tanto a la primera como segunda línea de defensa, revisión de las evidencias aportadas y seguimiento a la materialización de riesgos

Fuente: propia

Una vez se realice la designación de los roles y los usuarios que deben hacer parte de estos, se deberá realizar mesa de trabajo para la identificación y/o actualización de los riesgos cualquiera que sea su tipología en la cual deberá asistir el líder del proceso y/o su delegado junto con la persona administradora del módulo de la gestión de riesgos.

Nota: la parametrización de cada uno de los riesgos y sus monitoreos deberán realizarse conforme la versión del aplicativo vigente en el Ideam, por lo que se construirá ABC para la gestión de riesgos, como un documento anexo a esta política.

III. Seguimiento a la Política de Administración de riesgos

La Oficina de Planeación es la encargada de liderar la gestión para implementar y efectuar el seguimiento, control y mejora continua de la presente política, la cual deberá revisarse al menos una vez al año con el fin de determinar su pertinencia, funcionalidad y realizando los ajustes necesarios en caso de requerirse.

Los instrumentos metodológicos se revisarán de acuerdo con la necesidad y en especial, atendiendo recomendaciones de organismos de control externo e interno, cuando se requieran implementar enfoques o sistemas de gestión que deban articularse con el sistema de control interno, la gestión integral de riesgos de la organización y como producto del análisis de contexto.

El seguimiento a la implementación y mejora de la gestión de riesgos del Ideam se desarrollará de acuerdo con los lineamientos definidos en esta política institucional, así como en los monitoreos y evaluaciones periódicas que desarrolla la segunda y tercera línea de defensa

IV. Comunicación y consulta

El consolidado de los mapas de riesgo se publicará en la página web de la entidad, link de transparencia, numeral 4 "Planeación".

Se deberá realizar la socialización del mapa de riesgos de corrupción de la entidad a servidores públicos y contratistas en diferentes espacios como lo son mesas de trabajo, capacitaciones de la administración del riesgo y en los comités de coordinación de control interno y comité de gestión y desempeño, durante la vigencia, con el fin de recibir observaciones para su mejora, así mismo, será publicada en la página web del Ideam para consulta y comentarios de la ciudadanía.

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.

Documentos relacionados

- Política de Planeación Institucional
- Política de Control interno
- Política de transparencia
- Política General de seguridad de la información
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Bibliografía

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

Control de cambios

Versión	**Fecha**	**Descripción**
01	27/06/2025	Se realiza cambio de la Guía de administración del riesgo Versión 6 (SGI-G003) a la Política de Administración del riesgo la cual fue aprobada el 27 de junio de 2025 en el Comité De Coordinación De Control Interno.

Elaboró	Revisó	Aprobó
Oficina Asesora de Planeación	Jefe de la Oficina Asesora de Planeación	Comité de Coordinación de Control Interno del 27 de junio de 2025