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 del modelo de operación por procesos con 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 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.

La gestión del riesgo inicia con el análisis del contexto institucional y la identificación de riesgos y oportunidades en cada proceso. 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. adicionalmente, se incorporan la metodología para la identificación y valoración de los riesgos de relacionados con la Gestión ambiental, el Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP (Integridad pública, Soborno, Fraude, Inadecuada gestión del conflicto de intereses, Corrupción, Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP).

La implementación de la guía 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

Fortalecer la capacidad institucional del IDEAM mediante la implementación de un modelo integral de administración del riesgo que permita identificar, analizar, valorar, tratar y monitorear los riesgos de gestión, fiscales, de seguridad de la información, ambiental y de integridad pública, contribuyendo al cumplimiento de los objetivos estratégicos y misionales del Instituto.

Objetivos específicos:

- Establecer lineamientos metodológicos para la identificación y valoración de riesgos institucionales.
- Definir mecanismos de seguimiento y monitoreo bajo el enfoque de líneas de defensa.
- Integrar la gestión del riesgo con el direccionamiento estratégico, el MIPG y los sistemas de gestión institucionales.
- Fortalecer la gestión de riesgos de seguridad de la información y continuidad del negocio.
- Mitigar los impactos negativos que puedan generarse en el cumplimiento de la misionalidad de la entidad.

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 implementar adecuadamente el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP y a su vez identificar, analizar, valorar, tratar y monitorear los riesgos de gestión, de integridad pública, fiscales, ambientales 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 equipos de trabajo, 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. Para los riesgos que se encuentran en un nivel diferente a bajo, se deben establecer controles e indicadores de acuerdo con su residualidad y realizar el seguimiento de manera periódica.

Para los riesgos ambientales se contará con la identificación de los aspectos e impactos ambientales, siendo esta la línea base de identificación, valoración y establecimiento de controles operacionales, una vez se identifiquen los impactos ambientales que puedan generar una afectación en la operación y misionalidad de la entidad, estos serán identificados en la matriz de riesgos de acuerdo con el proceso.

Modelo Institucional de Gestión Integral del Riesgo

Constituye el marco mediante el cual la entidad articula los componentes estratégicos, metodológicos y operativos necesarios para administrar de manera integral los riesgos que puedan afectar el cumplimiento de su misión, la generación de valor público, la continuidad de la operación científica y técnica, la transparencia, la integridad y el logro de los objetivos institucionales.

Este modelo materializa los lineamientos establecidos en la Política de Administración Integral del Riesgo y se desarrolla a través de la presente Guía, la cual integra seis componentes que interactúan de manera permanente dentro de un ciclo de mejora continua. Cada componente cumple un propósito específico, pero su efectividad depende de la articulación con los demás, permitiendo que la gestión del riesgo deje de ser una actividad aislada para convertirse en un elemento transversal del direccionamiento estratégico y de la gestión institucional.

Ilustración 01 Modelo Institucional de Gestión del Riesgo

Fuente: propia 2026

La implementación del modelo inicia con la **identificación del contexto**, entendido como el análisis sistemático de los factores internos y externos que pueden influir en el cumplimiento de la misión institucional. Este análisis comprende aspectos estratégicos, normativos, tecnológicos, ambientales, científicos, financieros, sociales y territoriales, así como las necesidades y expectativas de las partes interesadas. La comprensión del contexto permite identificar oportunidades, amenazas y riesgos emergentes, constituyendo la base para la toma de decisiones y la priorización de los riesgos institucionales.

A partir del conocimiento del contexto, se integran los **instrumentos de planeación estratégica**, mediante los cuales la gestión del riesgo se incorpora al direccionamiento institucional, asegurando su alineación con el Plan Estratégico Institucional, los planes de acción, los proyectos de inversión, las políticas institucionales, el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno (MECI) y los demás sistemas de gestión implementados por la entidad. Esta articulación garantiza que la administración del riesgo contribuya directamente al logro de los objetivos estratégicos y no se limite únicamente al cumplimiento de un requisito metodológico.

Como complemento al componente estratégico, el modelo incorpora los **instrumentos de contingencia**, orientados a fortalecer la capacidad institucional para responder oportunamente frente a la materialización de riesgos, incidentes de seguridad de la información, eventos de continuidad

operativa, emergencias y demás situaciones que puedan afectar la prestación de los servicios o el cumplimiento de la misión institucional. Estos instrumentos permiten que la administración del riesgo trascienda el enfoque preventivo e incorpore capacidades de preparación, respuesta, recuperación y aprendizaje institucional.

Con base en los elementos anteriores, el **Marco Metodológico para la Gestión del Riesgo** proporciona los lineamientos técnicos para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos de gestión, fiscales, ambientales, de seguridad de la información, integridad pública y demás tipologías definidas por la entidad. Este componente establece criterios homogéneos para la administración del riesgo, asegurando la aplicación de metodologías consistentes en todos los procesos y fortaleciendo la comparabilidad, trazabilidad y consolidación de la información institucional, se consolida principalmente a través del mapa institucional de riesgos.

La adecuada implementación del modelo requiere, además, la definición de **procedimientos y protocolos para la administración del riesgo**, mediante los cuales se establecen las actuaciones específicas frente a situaciones particulares que requieren un tratamiento diferenciado, tales como el programa de transparencia y ética de lo público -PTEP, Manual de debida diligencia, procedimiento atención canal de denuncias y demás actuaciones necesarias para garantizar respuestas oportunas y coordinadas en todos los niveles de la organización.

Finalmente, el modelo se consolida mediante los **instrumentos de planeación, seguimiento y mejora continua**, los cuales permiten evaluar periódicamente la efectividad del Sistema Integral de Gestión del Riesgo a través del monitoreo de indicadores clave de riesgo (KRI), el seguimiento a los planes de tratamiento, el análisis de materializaciones, la evaluación de la madurez institucional, las auditorías, la autoevaluación y la revisión por la Alta Dirección. Los resultados obtenidos retroalimentan el análisis del contexto institucional, promoviendo la actualización permanente de los riesgos, el fortalecimiento de los controles y la mejora continua del sistema.

De esta manera, el Modelo Institucional de Gestión Integral del Riesgo se configura como un proceso dinámico, cíclico y articulado, en el que cada uno de sus componentes fortalece a los demás y permite que la gestión del riesgo haga parte integral de la gobernanza institucional la cual está definida en la Política de Administración del Riesgo. Su implementación contribuye al fortalecimiento de la capacidad institucional para anticipar eventos, gestionar la incertidumbre, tomar decisiones informadas y proteger la misión del Ideam, promoviendo una

cultura organizacional basada en la prevención, la integridad, la resiliencia y la generación sostenible de valor público.

Definiciones

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.
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 inmediata: situación que facilita la ocurrencia del riesgo.

Causa raíz: origen principal que genera el riesgo

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.

Control en ISO 27001: Es una medida o mecanismo (política, procedimiento, práctica o tecnología) que se implementa para reducir riesgos y proteger la seguridad de la información dentro de una organización.

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.

Integridad para la información: Es la propiedad que garantiza que la información sea exacta, completa y no haya sido modificada de manera no autorizada (seguridad de la información)

Impacto ambiental: Alteración del medio ambiente, positiva o negativa, ocasionada por los aspectos ambientales asociados a las actividades, productos o servicios de una organización, que puede afectar componentes como el aire, el agua, el suelo, la flora, la fauna, los recursos naturales o la salud y bienestar de las personas.

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 ambiental: Efecto de la incertidumbre asociado a los aspectos ambientales de una organización, que puede ocasionar impactos adversos sobre el medio ambiente, afectar el cumplimiento de los requisitos legales y otros requisitos aplicables, comprometer el logro de los objetivos ambientales o generar consecuencias para la organización y sus partes interesadas.

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
- LA/FT/FT: Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP)
- 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.
- **Decreto 1078 de 2015.** Es el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia.
- **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 27001:2022.** Estándar internacional para Sistemas de Gestión de Seguridad de la Información (SGSI). Controles Anexo A.
- **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.
- **Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas:**
  Documento que amplia y profundiza en los contenidos presentados en la guía de gestión de riesgos del DAFP relacionados con el análisis del contexto, con un énfasis especial en el entorno digital. Aborda la identificación de activos, la elaboración de catálogos de amenazas y vulnerabilidades para el análisis exhaustivo de los riesgos de seguridad de la información.
- **Ley 1273 de 2009 Delitos informáticos:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Esta Ley en el Artículo 269H incluye Circunstancias de agravación punitiva cuando hay fines terroristas o genera riesgo para la seguridad o defensa nacional.
- Normativa aplicable para seguridad de la información o aspectos jurídicos que apliquen directa o indirectamente al IDEAM, para cada uno de los riesgos identificados: Ley 1581 de 2012, sobre protección de datos

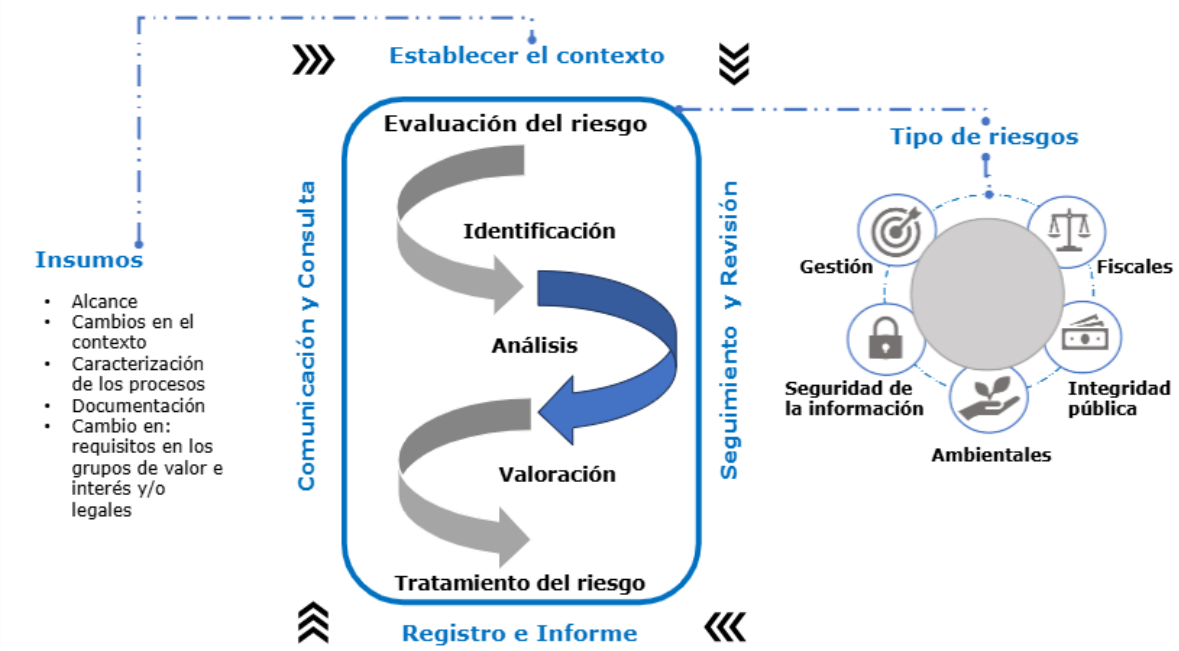
personales, Ley 1712 de 2014 sobre transparencia de la información, circulares o regulaciones emitidas por superintendencias o ministerios, como el Decreto 1078 de 2015 sobre el reglamento en tecnología de la información, el Decreto número 1083 de 2015, modificado por el Decreto 1499 de 2017, sobre norma que reglamenta y actualiza el Modelo Integrado de Planeación y Gestión (MIPG) en Colombia.

Metodología para la administración integral del riesgo

El Ideam, en cumplimiento de su función como entidad pública, establece en el presente documento la metodología para la implementación y aplicación de la Política Integral para la Administración del Riesgo, con fundamento en los lineamientos definidos por el Departamento Administrativo de la Función Pública (DAFP) en la versión vigente de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Esta metodología adopta los principios y criterios establecidos para la gestión de los riesgos de gestión, seguridad de la información, ambientales, fiscales e integridad pública, adaptándolos al contexto, necesidades y características institucionales del Ideam, y define las directrices para una gestión integral, sistemática y efectiva del riesgo.

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 en la ilustración 2 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

Contexto

Es este sentido, se inicia con la identificación de los insumos, como el alcance, caracterización de los procesos, documentación, cambios en los requisitos de valor e interés, aspectos impactos ambientales, así como la identificación del contexto de la Entidad determinando un análisis estratégico sea visto de manera integral (SGI-M008 Manual de operación del Modelo Integrado de Planeación y Gestión MIPG), dado que las políticas y dimensiones que lo integran se articulan de manera directa con una adecuada gestión por procesos.

La gestión por procesos se constituye en el eslabón que conecta la planeación estratégica de cualquier entidad con el despliegue de la parte operativa. Para

ello, toma como insumos algunos elementos de la dimensión de direccionamiento estratégico en la medida en que debe alinearse con la misión, visión y objetivos estratégicos, entre otros.

Para efectos del SIGRIP, ese contexto debe complementarse con los siguientes análisis[1]:

a) La planta y estructura de la entidad, así como la delegación de autoridad o poder decisorio discrecional dentro de la organización. Para estos efectos, podrá remitirse al mapa de redes internas, al modelo de gobernanza o a la matriz de atribuciones y decisiones, que haya desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.

b) Los grupos de valor o partes interesadas, incluidos los clientes internos y externos. Se debe hacer especial énfasis en identificar aquellos que pueden considerarse contrapartes, es decir, partes con las que se tienen interacciones, entendidas estas como cualquier tipo de vinculación que involucre la prestación o entrega de un producto, o el intercambio de recursos.

c) Si la entidad está desconcentrada en el país, identificar los lugares en qué opera. Así mismo, si por su misión, opera en otras jurisdicciones o en sectores, industrias o mercados específicos, identificarlos.

d) La naturaleza, escala y complejidad de los procesos, servicios, trámites u otras operaciones administrativas de la organización. Dentro de este análisis deben incluirse e identificarse todas las interacciones, es decir, las operaciones con contrapartes que involucran la prestación o entrega de un producto, o el intercambio de recursos.

e) Información general sobre los contratos y principales proveedores de la entidad. Este análisis implica agrupar a los contratos y proveedores según características como: naturaleza jurídica, modalidad de selección más recurrente, valores mínimos, máximos y media de contratación, relación de cumplimiento o incumplimientos, tipos de supervisión, entre otras variables que pueda construir la entidad para conocer a sus proveedores.

f) Las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización. Para estos efectos podrá remitirse al mapa de redes externas o al modelo de relacionamiento, que haya

[1] Tomado de la Guía de Administración del Riesgo versión 7 DAFP 2025

desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.

g) La naturaleza y alcance de las interacciones con entidades de otras Ramas del Poder Público, órganos de control o independientes. Así como de las interacciones con particulares que no derivan en un vínculo formal, pero que son recurrentes (actividades de cabildeo). Para estos efectos podrá remitirse al mapa de redes externas o al modelo de relacionamiento, que haya desarrollado en el marco de la temática de Redes y Articulación del Programa de Transparencia y Ética Pública.

h) Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales. Agrupando entre aquellas que son deberes (obligatorio cumplimiento), expectativas (cumplimiento facultativo) y compromisos (cumplimiento asumido). Para esto podrá remitirse al Marco Normativo que tenga disponible según lo establecido en materia de Transparencia y Acceso a la Información Pública.

Riesgos emergentes

El Ideam reconoce que la gestión del riesgo debe evolucionar de manera permanente para responder a los cambios del entorno, a las nuevas amenazas y a las lecciones aprendidas derivadas de la operación institucional.

En este sentido, los **riesgos emergentes** corresponden a aquellos eventos potenciales cuya probabilidad de ocurrencia, impacto o nivel de exposición puede incrementarse como consecuencia de cambios en el contexto interno o externo de la Entidad, así como por la identificación de nuevas causas derivadas de procesos de evaluación, auditoría, seguimiento o análisis institucional.

Estos riesgos pueden afectar el cumplimiento de la misión institucional, la prestación de los servicios científicos y técnicos, la continuidad de la operación, la seguridad de la información, la integridad pública, el cumplimiento normativo, el patrimonio institucional o la generación de valor público, razón por la cual deberán ser objeto de identificación, análisis y gestión oportuna.

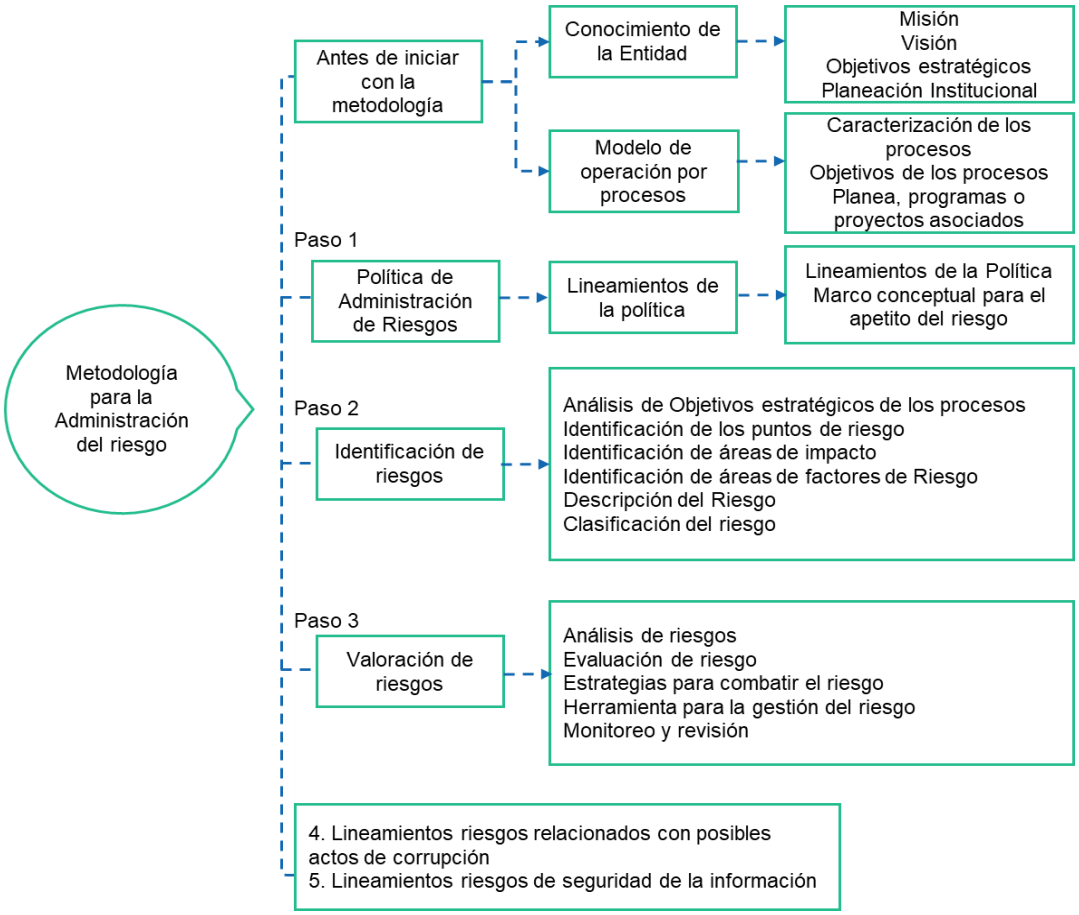
La identificación de riesgos emergentes constituye un mecanismo preventivo que fortalece la capacidad institucional para anticiparse a escenarios futuros y adoptar decisiones antes de que los riesgos se materialicen.

Los riesgos emergentes podrán originarse, entre otros, a partir de las siguientes fuentes de información:

- Cambios en el contexto estratégico.
- Hallazgos y oportunidades de mejora identificadas en auditorías internas.
- Hallazgos, observaciones o recomendaciones formuladas por organismos de control, entes certificadores o auditorías externas.
- Materialización de riesgos institucionales.
- Incidentes de seguridad de la información.
- Cambios en la operación institucional o en la prestación de servicios.
- Cambios tecnológicos o incorporación de nuevas herramientas.
- Modificaciones normativas.
- Nuevos proyectos, procesos o servicios institucionales.
- Quejas, denuncias, PQRSD y demás mecanismos de participación ciudadana.
- Resultados del seguimiento a indicadores clave de riesgo (KRI).
- Evaluaciones de la matriz de madurez del Sistema Integral de Gestión del Riesgo.
- Lecciones aprendidas derivadas de contingencias, emergencias o eventos críticos.

Una vez analizado lo anterior, se estructura la metodología aplicada para la administración de riesgos de gestión, fiscales, seguridad de la información, ambiental y de integridad pública se evidencia en la ilustración 3 a continuación:

Ilustración 3 Metodología para aplicar correctamente la administración del riesgo



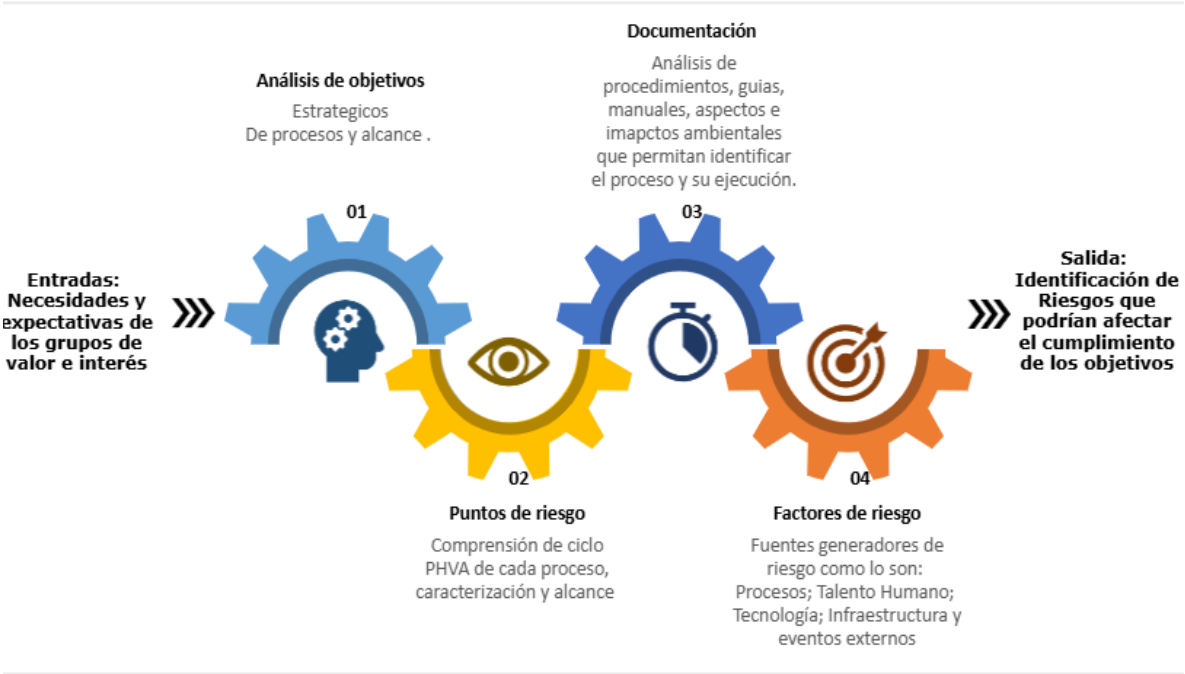
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas 2022

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 en la ilustración 4:

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], los cuales se describen a continuación en la tabla 1:

[2] NTC ISO 31000, Numeral 2.9

Tabla 1 Listado de Factores

Factor	Definición	Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	• Falta de aplicación de los procedimientos • Falta segregación de funciones • Errores de grabación, autorización • Falta de supervisión o interventoría • Errores en cálculos para pagos internos y externos • Alta rotación o insuficiencia de personal • Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo • Acciones contrarias a las leyes o acuerdos contractuales • Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	• Contrapartes de la entidad (naturales o jurídicas) • Productos (bienes o servicios) que oferta/requiere • Canales utilizados para la operación • Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos	• Fraude Interno • Soborno

Factor	Definición	Descriptores
	de los empleados que afectan la Integridad Pública.	• Gestión inadecuada de conflicto de Intereses • Corrupción • Hurto activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	• Daño de equipos • Caída de sistemas de información y aplicaciones • Caída de redes • Errores en hardware o software • Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	• Derrumbes • Incendios • Inundaciones • Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.	• Fraude Externo • Suplantación de identidad • Asalto a la oficina • Atentados, vandalismo, orden público
Ambiental	Acciones desarrolladas que pueden generar un impacto al medio ambiente	• Contaminación del recurso aire • Contaminación del suelo • Contaminación del agua • Generación de CO2

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional -Función Pública y Secretaría de Transparencia, 2025.

Para el caso de los riesgos emergentes la Oficina Asesora de Planeación consolidará la información proveniente de: auditorías internas; auditorías externas; auditorías de certificación; auditorías realizadas por organismos de control; evaluaciones independientes; seguimientos efectuados por la Oficina de Control Interno, desviaciones relevantes de indicadores; resultados de planes de mejoramiento; reportes de eventos operacionales; reclamaciones y PQRSD; entre otros insumos que puedan identificar tendencias, hallazgos recurrentes, debilidades sistémicas y oportunidades de mejora que puedan representar nuevos riesgos para la Entidad.

Con este insumo se deberá convocar mesas de trabajo con la participación de la primera línea de defensa, con el propósito de realizar un análisis estructurado de las situaciones identificadas, en donde se debe:

- analizar las causas raíz de los hallazgos o situaciones identificadas;
- validar si las causas corresponden a riesgos existentes o evidencian nuevos riesgos;
- identificar tendencias o patrones repetitivos;
- evaluar los controles actuales;
- determinar si existen riesgos transversales que afecten más de un proceso;
- establecer la tipología de riesgo que corresponda de acuerdo con la clasificación institucional (gestión, integridad pública, fiscal, seguridad de la información, ambiental u otras adoptadas por la Entidad);
- definir las acciones que permitan prevenir la materialización de nuevos riesgos.

Cuando el análisis determine la existencia de un nuevo riesgo, este deberá incorporarse en el mapa institucional siguiendo la metodología establecida en la presente Guía.

1.2 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 relacionada en la tabla 2:

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 infraestructura o por la ocurrencia de acontecimientos externos.

Tipo de riesgo	Descripción
	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 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 potencial. (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).
Riesgos ambientales	Posibilidad de que un aspecto ambiental genere un impacto negativo sobre el medio ambiente de forma significativa, debido a la ocurrencia de un evento o condición, considerando la probabilidad de que ocurra y la magnitud de sus consecuencias.
Riesgos de integridad pública	
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.

[3] Norma técnica de la calidad del proceso estadístico, requisitos de calidad para la generación de estadísticas - NTC PE 1000:2020

Tipo de riesgo	Descripción
Riesgo de soborno	El Soborno puede ser entendido como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]"9. Y opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.
Riesgo de Fraude	El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima. El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.
Conflicto de interés	Surge cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.
Riesgo de Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación	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.

Tipo de riesgo	Descripción
de Armas de Destrucción Masiva.	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas 2025

1.3 Descripción del riesgo

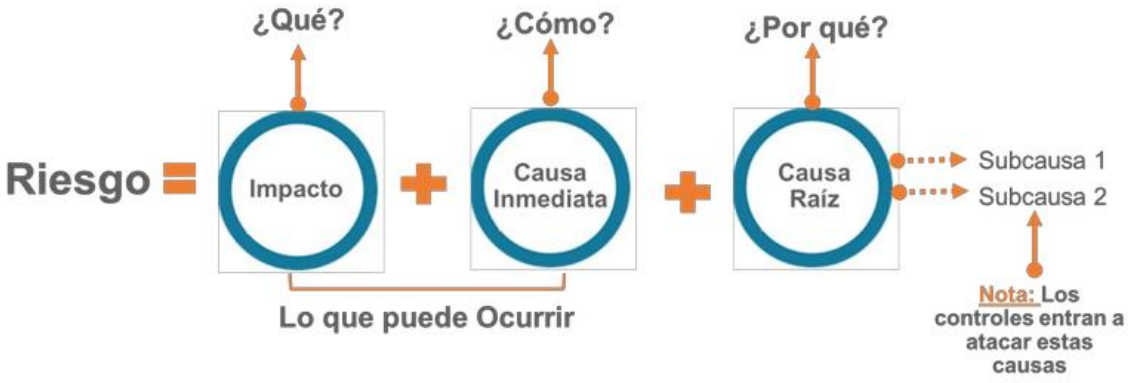
La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento, tanto para el líder del proceso como para personas ajenas al proceso.

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

1.3.1 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 7

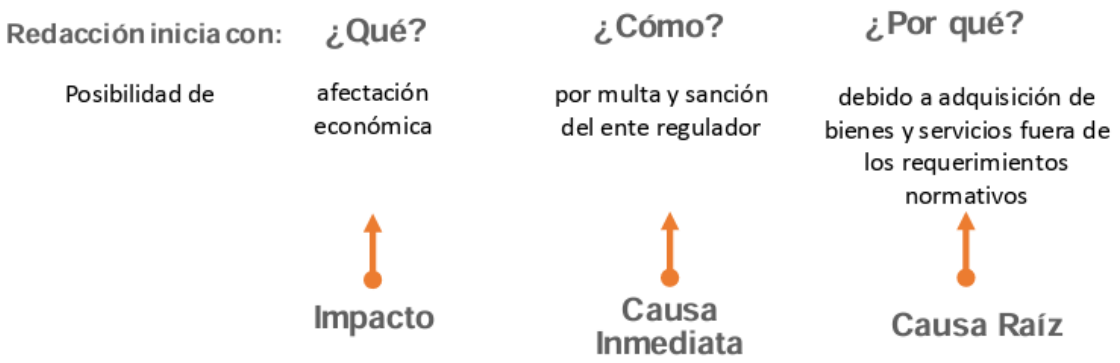
La redacción descrita permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y su causa raíz, siendo esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

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.

1.3.2 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.

El efecto económico del riesgo fiscal es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público.

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

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

- ✓ Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
- ✓ Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público
- ✓ Multas impuestas por hechos que no comportan gestión fiscal
- ✓ Existencia de actuación de cobro coactivo por parte de la entidad.
- ✓ Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.
- ✓ Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su "normal uso" (máquinas eléctricas, computadores, celulares, etc.). (Contraloría General de la República, 2023, p. 12).

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.

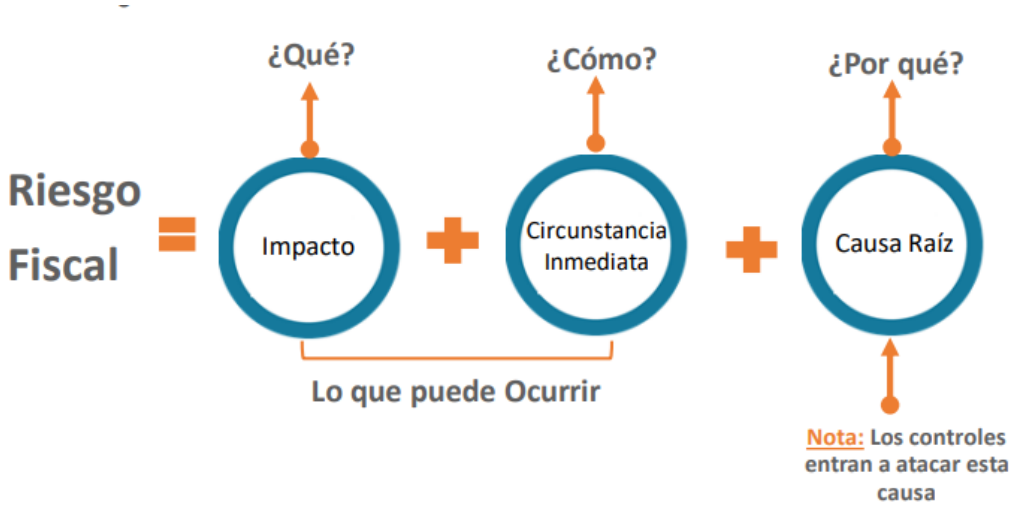
Y la causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

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, 2025

A continuación, en la tabla 3 se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso.

Tabla 3 Ejemplos de redacción de acuerdo con el objeto sobre el cual recae la posibilidad de efecto dañoso

Bienes públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la implementación y operación de redes eléctricas seguras.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por negación del reconocimiento de siniestros en el contrato de seguro, a causa de la omisión en la actualización del inventario de bienes amparados.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

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

1.3.3 Riesgos de Seguridad de la Información

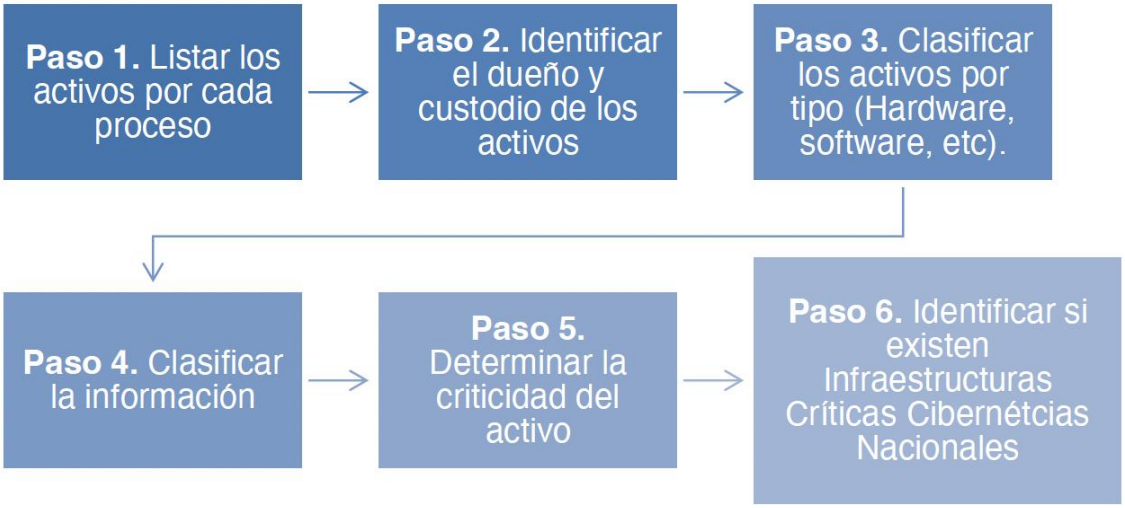
Se debe tener en cuenta el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura MRAE y soporta transversalmente los otros habilitadores de la política de gobierno digital.

Como primer paso para la identificación de riesgos de seguridad de la información, es necesario identificar y actualizar los activos de información de los procesos de la entidad. Esta identificación y valoración debe ser realizada por

la Primera Línea de Defensa - líderes de proceso, con la debida orientación del responsable de seguridad de la información del Instituto.

Por lo anterior, se deben seguir los siguientes pasos para la identificación y establecimiento de dichos activos:

Ilustración 8 Pasos para identificar activos de la información



Fuente: Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, MINTIC.

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, 2025

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.

Tipo de Vulnerabilidad

Una vulnerabilidad se refiere a toda aquella debilidad que puede presentar un activo de información, la cual puede ser explotada o usada por intrusos o atacantes comprometiendo la confidencialidad, integridad o disponibilidad de la información.

Tabla 5: Tipo de vulnerabilidad

Tipo de Vulnerabilidad	Descripción

Hardware	Se refiere a fallos o puntos débiles en los equipos físicos, como computadoras, servidores o dispositivos de red. Estas vulnerabilidades pueden permitir daños físicos, robos o accesos no autorizados a los sistemas.
Software	Se refiere a fallos o debilidades en los programas informáticos, que pueden ser explotados para obtener acceso no autorizado, alterar funcionalidades o causar incorrecto funcionamiento del sistema.
Red	Son vulnerabilidades en los métodos y políticas diseñados para proteger la información. Pueden incluir fallos en la implementación de controles de seguridad, políticas inadecuadas o falta de seguimiento de las mejores prácticas de seguridad.
Personal	Se refiere a riesgos asociados con las personas que tienen acceso a los sistemas e información. Pueden incluir falta de capacitación, errores humanos o incluso acciones malintencionadas de funcionarios o contratistas.
Instalaciones / Infraestructura física	Son debilidades en la seguridad de los espacios físicos donde se encuentran los sistemas informáticos, como edificios o centros de datos. Pueden incluir problemas con el control de acceso, protección contra incendios o desastres naturales.
Organización	Son puntos débiles en los procedimientos y flujos de trabajo de la organización. Estas vulnerabilidades pueden llevar a errores humanos, inconsistencias o brechas de seguridad debido a la falta de controles adecuados.

Fuente: Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, MINTIC 2025.

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 27005:2022 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.

Tipo de Amenaza

Se considera como amenaza (causa) cualquier agente externo al activo que puede aprovechar una vulnerabilidad de este para causar daño y que afectará la seguridad de la información. La identificación de amenazas se realiza mediante la evaluación de fuentes de información como:

- Criterio de expertos: Experiencia de los dueños, propietarios o equipo interdisciplinario que realiza la gestión de riesgo de los activos que se están evaluando.
- Bases de datos públicas sobre amenazas de seguridad de la información.

A continuación, se listan las posibles amenazas que pueden afectar los activos de información de acuerdo con su clasificación y origen.

Tabla 6: Tipo amenaza

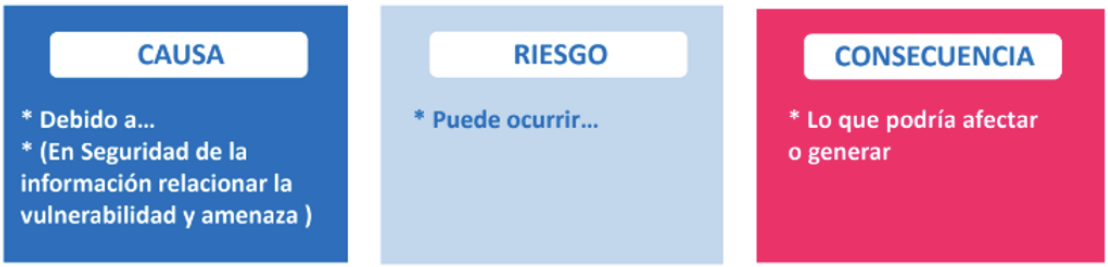
Tipo de Amenaza	Descripción
Amenazas físicas	Eventos que afectan directamente la infraestructura física donde se soportan los activos de información, como daños a equipos, accesos no autorizados a instalaciones, robo o vandalismo, que pueden comprometer la disponibilidad, integridad y confidencialidad de la información.
Amenazas naturales	Eventos de origen natural, tales como terremotos, inundaciones, incendios, tormentas o deslizamientos, que pueden causar interrupciones en la operación y pérdida de información o de infraestructura tecnológica.
Fallas en las infraestructuras	Interrupciones o fallos en los componentes de soporte tecnológico, como energía eléctrica, redes de telecomunicaciones, climatización o centros de datos, que afectan la continuidad y disponibilidad de los servicios de información.

Tipo de Amenaza	Descripción
Fallas técnicas	Errores o fallos en hardware, software o sistemas de información, tales como errores de configuración, fallas de sistemas operativos, corrupción de datos o fallos en aplicaciones, que pueden generar pérdida o alteración de la información.
Acciones humanas	Eventos derivados de acciones intencionales o no intencionales por parte de personas, como errores operativos, uso indebido de la información, negligencia, fraude, sabotaje o ataques cibernéticos, que pueden afectar la seguridad de la información.
Compromiso de funciones o servicios	Situaciones en las que los servicios tecnológicos o procesos críticos se ven afectados o interrumpidos, ya sea por ataques, fallas o accesos no autorizados, impactando la operación normal de la entidad.
Amenazas a la organización	Factores internos o externos que afectan la estructura, gobernanza o cumplimiento de la organización, como cambios normativos, falta de políticas, debilidades en la gestión, o incumplimiento de requisitos legales y regulatorios en seguridad de la información.

Fuente: Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, MINTIC 2025.

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

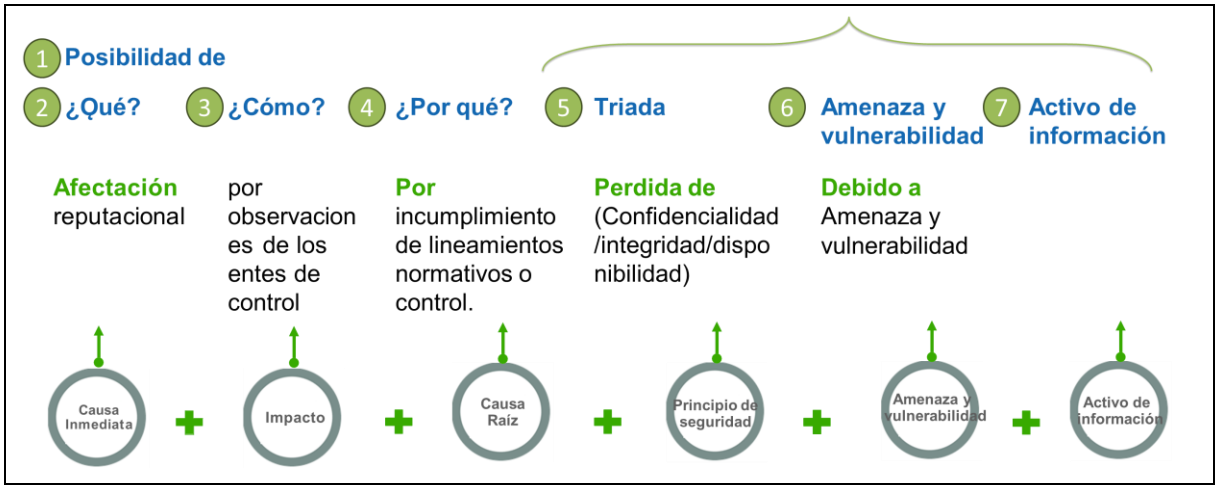


Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

Para la etapa de valoración de los riesgos se tomará como base lo definido en NTC ISO 27005:2022. 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.

En ese orden de ideas, los riesgos deben tener la siguiente estructura:

Ilustración 10 Redacción riesgos de seguridad de la información



Fuente: Creación propia basada en la metodología de gestión de riesgos DAFP

Ejemplo:

Posibilidad de afectación económica, reputacional, legal y operativa, debido a la pérdida de disponibilidad de servicios tecnológicos críticos, infraestructura, aplicaciones e información, como consecuencia de debilidades en el seguimiento y ejecución del Plan de Recuperación ante Desastres (DRP), lo que podría

generar incumplimiento de lineamientos y buenas prácticas de continuidad del negocio y seguridad de la información.

Nota: Los procesos misionales deben evaluar si cuentan con infraestructura crítica cibernética, de acuerdo con los Lineamientos para la identificación de infraestructuras críticas cibernéticas del MinTIC. Aquella infraestructura que sea identificada como crítica deberá contar obligatoriamente con una gestión de riesgos de seguridad de la información asociada.

Nota: Para los activos de información asociados a bases de datos que contienen datos personales, se deberán considerar adicionalmente los siguiente; pérdida de confidencialidad por divulgación no autorizada o uso indebido de la información; pérdida de integridad por alteración o modificación no autorizada de los datos; afectación a la disponibilidad de las plataformas tecnológicas o aplicativos que gestionan dichos datos; y la posibilidad de sanciones derivadas del incumplimiento de la normatividad vigente en materia de protección de datos personales.

1.3.4 Riesgos de integridad pública

La Organización para la Cooperación y el Desarrollo Económico, ODCE, ha planteado la necesidad de aplicar un enfoque basado en riesgos cuando se habla de integridad pública. Hay varias amenazas que pueden incidir en diferentes puntos de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en particular, asegurar el cumplimiento de la ley. Para el propósito de esta guía, nos centraremos en cinco amenazas para la integridad: corrupción, el soborno, el fraude, la inadecuada gestión del conflicto de intereses y el riesgo de LA/FT/FP.

En la guía de administración del riesgo versión 7 (2025), se recomienda tener en cuenta los siguientes ejemplos, los cuales son adoptados por el Ideam como referente para la identificación y análisis de este tipo de riesgos:

Tabla 7 Referentes para análisis del riesgo de integridad pública

Impacto	Causa Inmediata	Descripción de la causa inmediata	Causa Raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones	Descripción de la actividad en el flujo del proceso

Impacto	Causa Inmediata	Descripción de la causa inmediata	Causa Raíz
		incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	
Afectación económica y/o reputacional	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]".	Descripción de la actividad en el flujo del proceso
Afectación económica y/o reputacional	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona	Descripción de la actividad en el flujo del proceso

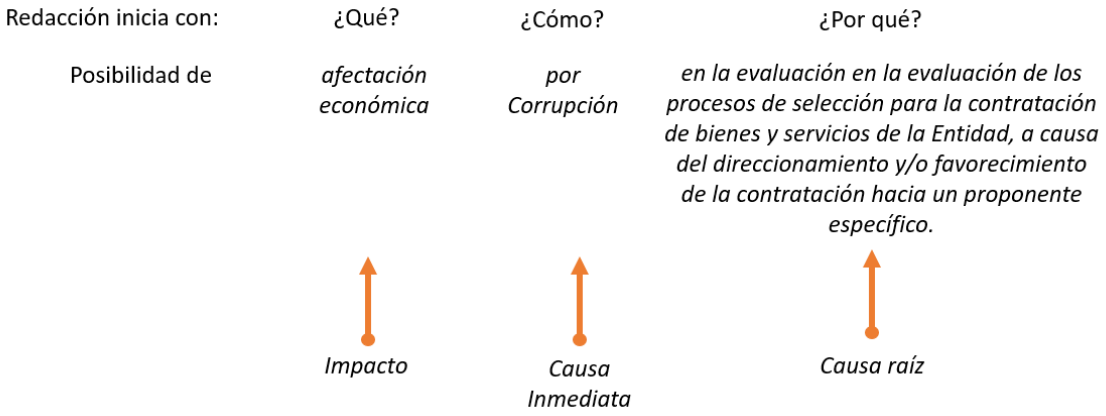
Impacto	Causa Inmediata	Descripción de la causa inmediata	Causa Raíz
		actúe o se abstenga de actuar […]".	
Afectación económica y/o reputacional	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	Descripción de la actividad en el flujo del proceso
Afectación económica y/o reputacional	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	Descripción de la actividad en el flujo del proceso

Fuente: adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025 (Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.)

Riesgo de corrupción

Cuando se habla de riesgos de corrupción se enfoca en desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero, por lo que a continuación se dará el ejemplo de la redacción de esta tipología de riesgo:

Ilustración 11 Redacción riesgo de corrupción



Fuente: Adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025

Riesgos de lavado de activos, financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva.

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

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

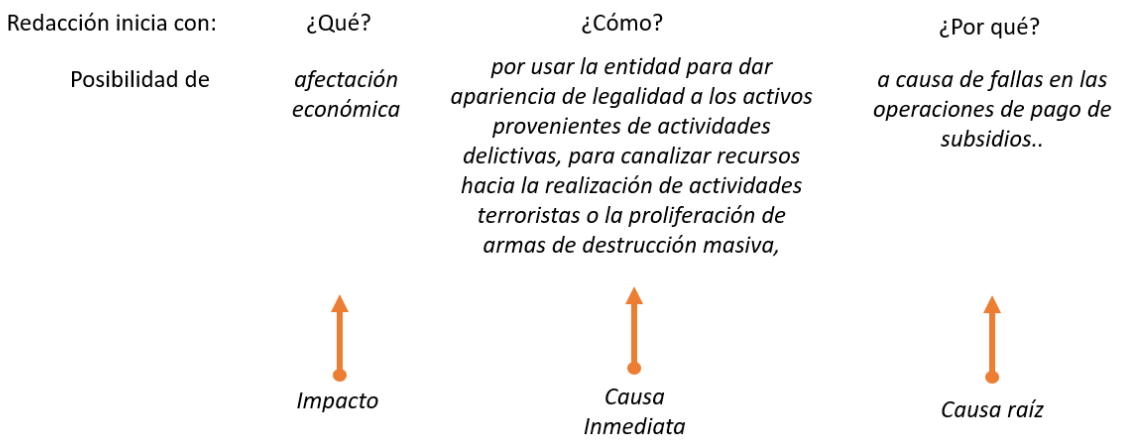
Teniendo en cuenta lo anterior, En el caso particular del riesgo LA/FT/FP, debe hacerse referencia particularmente a las actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo, como se explica en la tabla

Tabla 8 Análisis riesgos LA/FT/FP

Impacto	Causa inmediata	Causa raíz
Económico, Reputacional, Legal, Operativo o de Contagio	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva	Descripción de la Operación o Transacción

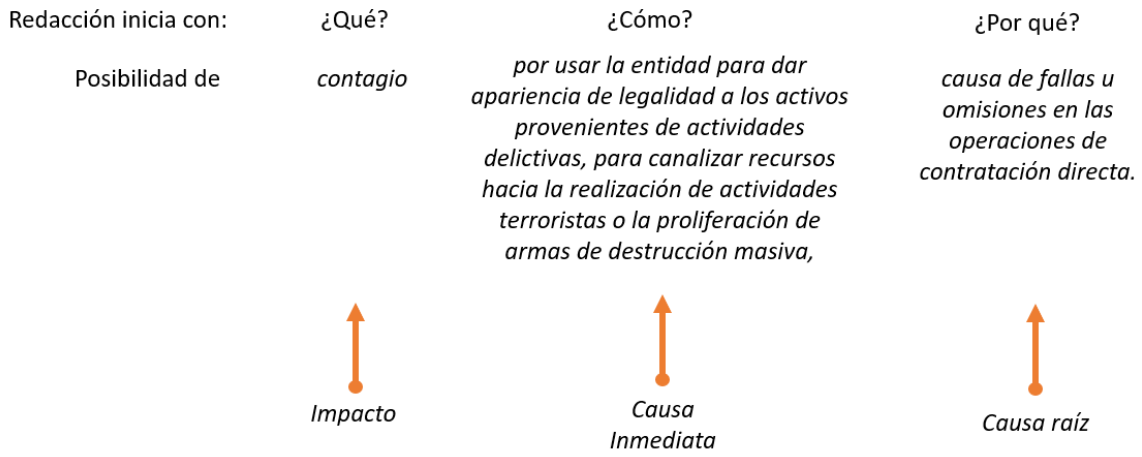
Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Ilustración 12 Ejemplo de redacción riesgo de LA/FT/FP



Fuente: Adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025

Ilustración 13 Ejemplo de redacción de riesgo LA/FT/FP por contagio



Fuente: Adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025

Por otro lado, para el diseño de controles deberá tenerse en cuenta que, además de la Política Integral para la administración del Riesgo y su respectivo Mapa de Riesgos, el Ideam deberá desarrollar, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, un Manual para el desarrollo del principio de debida diligencia, contar con una función de cumplimiento y formular una serie de herramientas de gestión.

Al final, estos elementos adicionales del Sistema son el repertorio de controles que tiene la entidad y que pueda aplicar en cada uno de los riesgos identificados, sin perjuicio de que puedan desarrollarse controles adicionales o muy específicos.

En todo caso, se sugiere que las políticas, procedimiento o códigos que se establezcan como controles se incorporen en la Política Integral para la gestión del Riesgo o en el Programa de Transparencia y Ética Pública, para asegurar la integralidad del Sistema.

Soborno

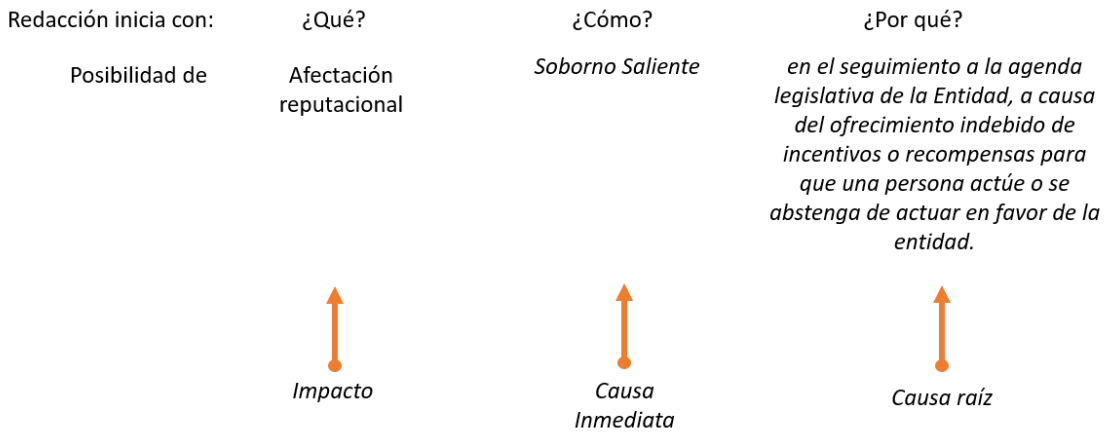
El Soborno puede ser entendido como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]"9. Y opera en dos niveles: Soborno Entrante y Saliente. Se entiende como Entrante el soborno al servidor de la Entidad, y

como Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

El Código Penal Colombiano tipifica el cohecho propio, el cohecho impropio, el cohecho por dar u ofrecer, todos estos delitos contra la administración pública, que son formas de soborno. Solamente entre particulares tipifica de forma general el soborno.

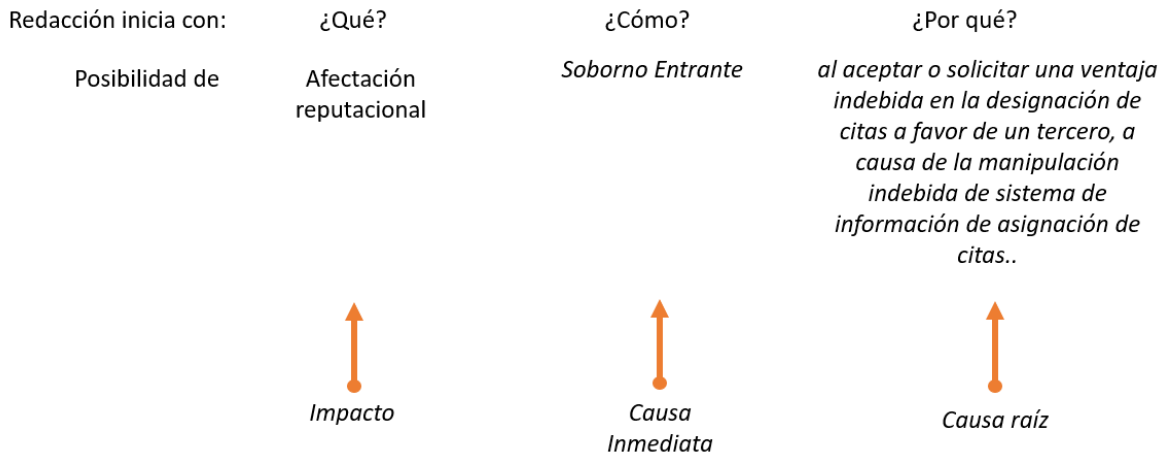
En este sentido, a continuación, se desarrollará un ejemplo de la redacción del riesgo de esta tipología:

Ilustración 14 Ejemplo de redacción de soborno saliente



Fuente: Adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025

Ilustración 15 Ejemplo de redacción de soborno saliente



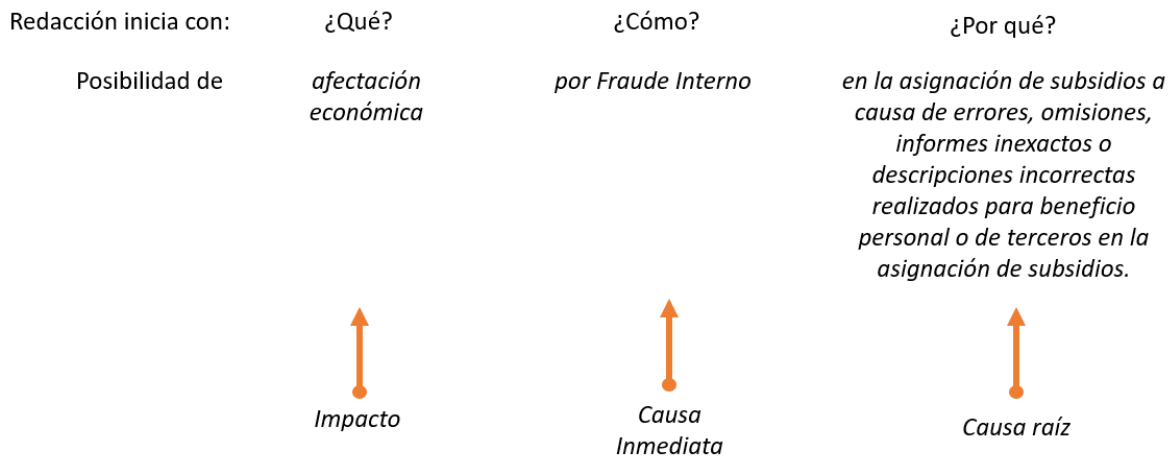
Fuente: Adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025

Fraude

El Fraude corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros10. Este puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima.

El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

Ilustración 16 Ejemplo de redacción de fraude interno



Fuente: Adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025

Inadecuada gestión del conflicto de intereses

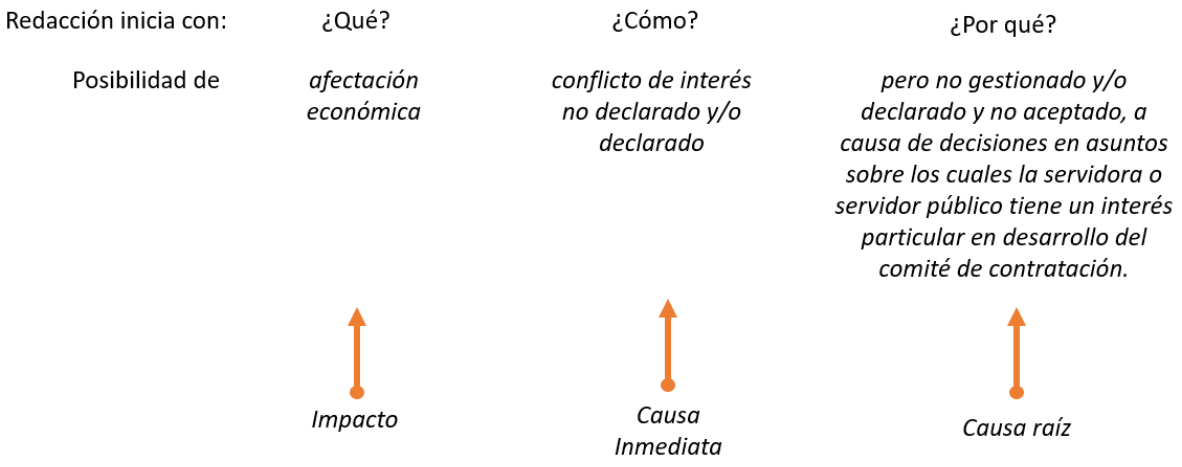
Un conflicto de intereses[4] surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación,

[4] Concepto construido a partir de lo establecido en el artículo 44 de la Ley 1952 de 2019, *"Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734*

gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.

Si bien la sola existencia del conflicto de intereses no implica una conducta reprochable, sí existen una serie de comportamientos definidos por códigos de conducta sobre la declaración y gestión del conflicto de intereses. La legislación nacional estima que quien tenga un interés particular en un asunto público está impedido para tomar la decisión.

Ilustración 17 Ejemplo de redacción para riesgos de conflicto de interés



Fuente: Adaptado de la Guía de administración del riesgo versión 7 DAFP, 2025

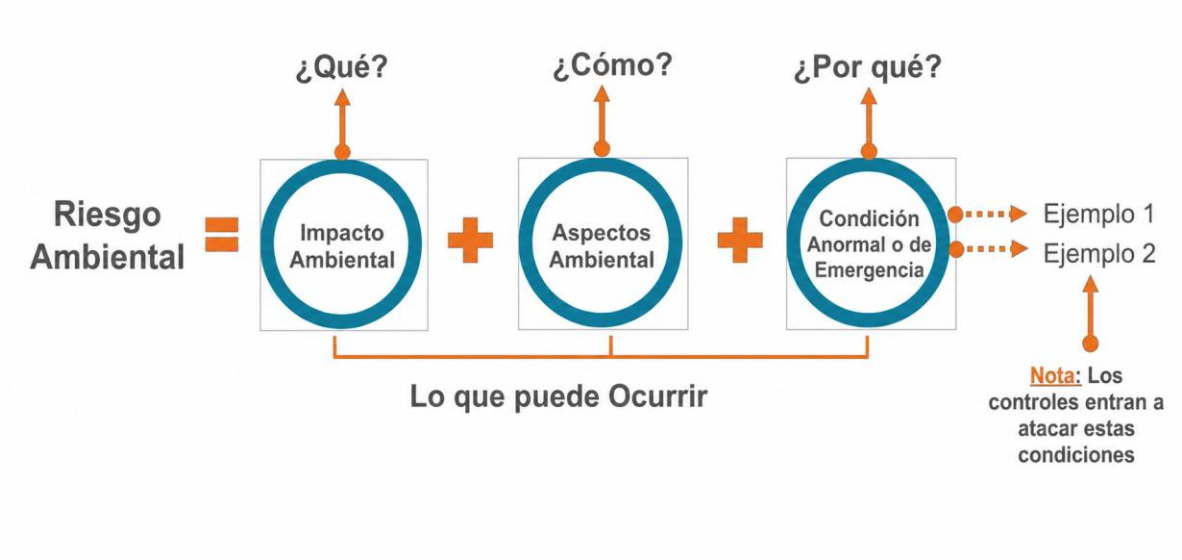
1.3.5 Riesgo ambiental

Para identificar los riesgos ambientales, se debe partir de la identificación de los aspectos e impactos ambientales por procesos, establecida en el formato SGI-F061 Matriz de identificación de aspectos y valoración de impactos ambientales, teniendo en cuenta el resultado de la valoración de este y si este se encuentra en condición anormal o de emergencia. Se propone una estructura que facilita

de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario"

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 18 Redacción riesgos ambientales



Fuente: propia 2026

La redacción del riesgo ambiental permite comprender qué puede ocurrir (impacto ambiental), cómo puede ocurrir (aspecto ambiental) y por qué puede ocurrir (condición anormal o de emergencia), facilitando la identificación de las causas asociadas y constituyéndose en información esencial para la definición de controles durante la etapa de valoración del riesgo.

De acuerdo con la gráfica presentada, el riesgo ambiental se estructura a partir de los siguientes elementos:

Impacto ambiental: Corresponde al efecto o consecuencia que puede generarse sobre el medio ambiente como resultado de la materialización del riesgo, por ejemplo: contaminación del suelo, agua o aire, afectación de la flora y fauna, agotamiento de recursos naturales o generación de molestias a la comunidad.

Aspecto ambiental: Es el elemento de las actividades, productos o servicios que interactúa o puede interactuar con el medio ambiente, tales como la

generación de residuos peligrosos, vertimientos, emisiones atmosféricas, consumo de agua o energía, almacenamiento de sustancias químicas, entre otros.

Condición anormal o de emergencia: Corresponde a la situación no rutinaria, falla, incidente o emergencia que puede desencadenar el riesgo ambiental, por ejemplo: derrames, fugas, incendios, explosiones, accidentes de transporte, fallas operacionales o eventos naturales.

Ejemplo: Posibilidad de afectación reputacional debido a la de contaminación del recurso suelo, por derrame o fuga de RESPEL generados por accidente durante el transporte hacia los sitios de tratamiento, aprovechamiento o disposición final.

1.3.6 Riesgos Transversales

Se desarrollará mediante un enfoque de coordinación institucional, en el cual se identificará un líder funcional del riesgo, encargado de orientar metodológicamente su administración y de emitir los lineamientos generales para su gestión.

La identificación podrá originarse a partir de: análisis del contexto institucional; auditorías internas o externas; seguimiento a riesgos institucionales; materialización de riesgos; mesas de trabajo interprocesos; cambios normativos; análisis de causas comunes; seguimiento de indicadores institucionales.

Cuando se evidencie que un mismo evento de riesgo afecta a varios procesos, la Oficina Asesora de Planeación convocará a mesa de trabajo y promoverá un análisis conjunto para determinar su carácter institucional y transversal, y se deberá realizar cada uno de los pasos para la identificación, evaluación, valoración y seguimiento de los riesgos definidos en esta guía.

Para cada riesgo transversal se identificará la dependencia responsable de emitir los lineamientos institucionales sobre la materia objeto del riesgo, esta dependencia ejercerá el liderazgo funcional del riesgo, independientemente del proceso donde se origine el evento.

En términos generales, el liderazgo recaerá sobre la dependencia que, en ejercicio de la segunda línea de defensa o de sus funciones institucionales, tenga la competencia para:

- formular políticas institucionales;

- emitir lineamientos técnicos;
- definir metodologías;
- establecer criterios de seguimiento;
- coordinar la implementación de acciones institucionales;
- orientar a los procesos sobre la administración del riesgo.

En consecuencia, la administración metodológica del riesgo transversal se verá reflejada en la dependencia que ejerza la segunda línea de defensa o que tenga asignada la responsabilidad institucional de emitir los lineamientos para la gestión y funcionamiento del tema asociado al riesgo.

Lo anterior no implica el traslado de la responsabilidad sobre la gestión del riesgo, la cual continuará siendo de la primera línea de defensa en cada uno de los procesos involucrados.

El líder funcional, en conjunto con los procesos involucrados, establecerá los controles institucionales comunes que deberán implementarse para reducir la exposición al riesgo.

Estos controles podrán incluir, entre otros:

- políticas institucionales;
- procedimientos;
- instructivos;
- protocolos;
- controles tecnológicos;
- mecanismos de supervisión;
- actividades de capacitación;
- indicadores institucionales;
- mesas técnicas de seguimiento.

Cada proceso incorporará estos controles dentro de sus actividades, de acuerdo con el nivel de responsabilidad que le corresponda.

La dependencia que ejerza el liderazgo funcional consolidará periódicamente la información suministrada por los procesos involucrados, con el propósito de evaluar:

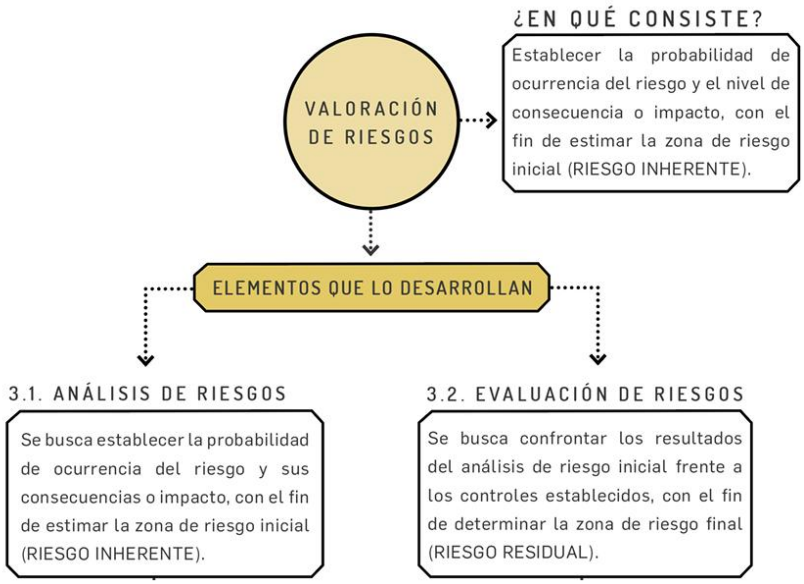
- la eficacia de los controles;
- monitorear el riesgo;
- el cumplimiento de las acciones;
- la necesidad de actualizar lineamientos institucionales.

- incorporar para su monitoreo indicadores clave de riesgo para ser llevados al CICCI, junto con las recomendaciones para la toma de decisiones estratégicas.

2. 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 19 Valoración del riesgo



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

2.1 Riesgo de Gestión, Fiscales, seguridad de la información y de integridad pública

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 9 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 20 Criterios para definir la probabilidad

	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 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 25 a 500 veces por año	**60%**

Alta	La actividad que conlleva el riesgo se ejecuta más de 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: Criterios para definir el nivel de probabilidad, DAFP. 2025.

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, sin embargo, para los riesgos de integridad pública NO podrán ser evaluados con los criterios de leve o menor, esto teniendo en cuenta que la afectación a la reputación de la entidad en caso de materialización no será menor.

Ilustración 21 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 2025

Nota: Para la seguridad de la información, en la identificación de los activos de información se evalúan la confidencialidad, integridad y disponibilidad, considerando su impacto en términos económicos, reputacionales, legales y de

afectación a los procesos u operaciones. En consecuencia, todos los activos con criticidad alta o extrema, así como aquellos identificados como infraestructura crítica cibernética, deben ser incluidos obligatoriamente en la gestión de riesgos de seguridad de la información.

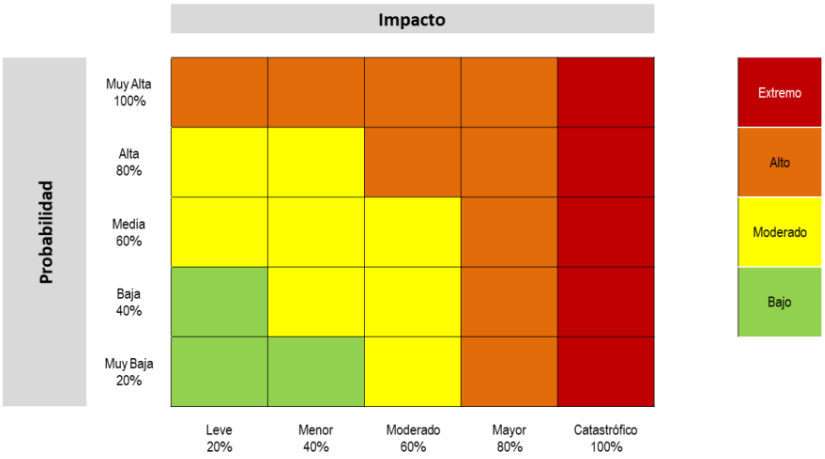
2.3 Evaluación de riesgo

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, para los riesgos de gestión, seguridad de la información y fiscales 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 22 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

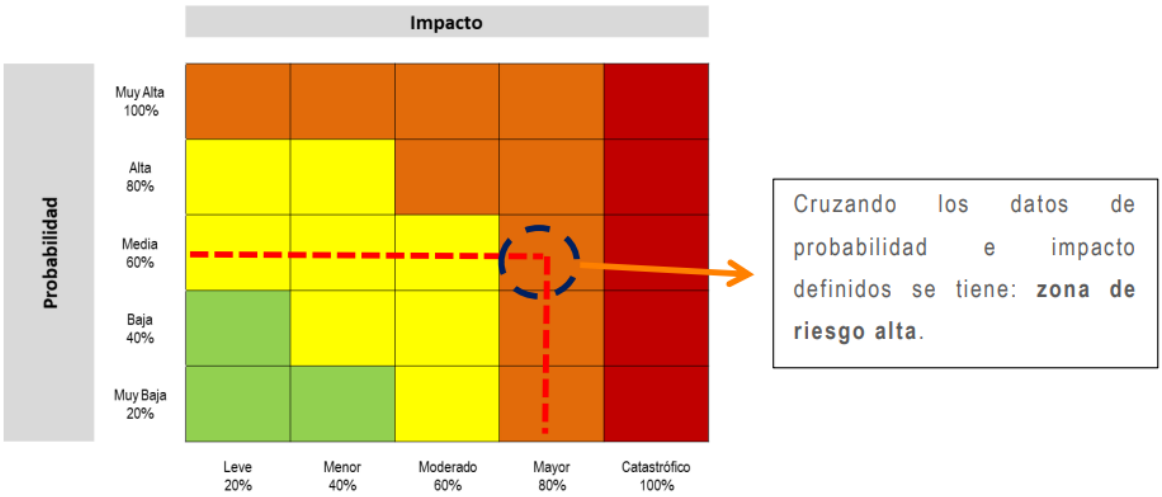
Riesgo identificado: Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

Probabilidad Inherente = Media 60%

Impacto Inherente: Mayor 80%

Aplicando el mapa de calor tenemos:

Ilustración 23 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 integridad pública no aplica el apetito ni la tolerancia al riesgo.

3. 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.

3.1 Estructura para la descripción del control

Se propone una adecuada redacción del control así:

Responsable+ Acción + Complemento

Responsable de ejecutar el control: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (Directores, asesores, profesionales, técnicos, asistenciales), así como su despliegue en grupos de trabajo internos e incluir coordinadores o gerentes de proyectos. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.

Su definición deberá igualmente considerar que éste cuenta con un nivel de autoridad apropiado de cara a la actividad de control, así como aspectos básicos de segregación de funciones para evitar que quién sea la fuente generadora de riesgo, sea el único que aplica alguna actividad de control.

Acción: Determina para qué se realiza el control, se utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.

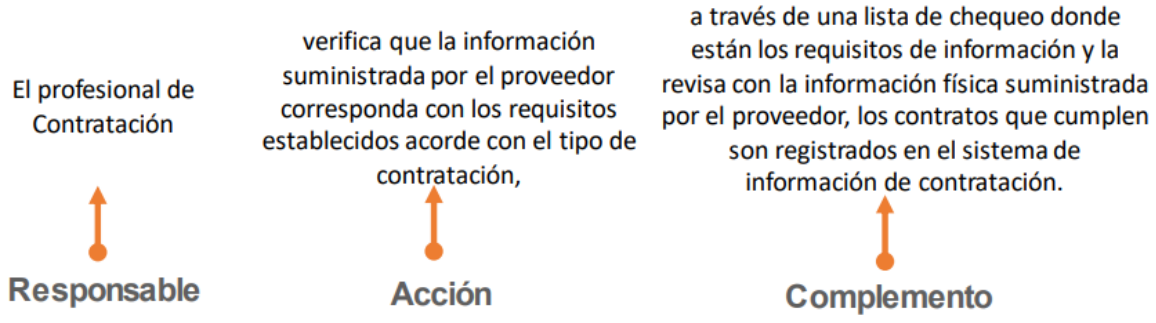
Complemento: corresponde a los atributos informativos o de formalización del control; corresponde a los detalles que permiten al responsable implementar el control, tal y como ha sido establecido o diseñado se contemplan los siguientes aspectos:

- ✓ Documentación: se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
- ✓ Frecuencia: corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
- ✓ Evidencia: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
- ✓ Ejecución: permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten. Puede darse a través de la comparación con información interna, externa o mixta.

Se tiene entonces que, para la redacción del control es necesario aplicar todos los atributos acá descritos, de manera tal que se constituyan en una herramienta de control efectiva, los cuales se agrupan a través de la estructura para la redacción del control.

A continuación, se establece un ejemplo con la estructura:

Ilustración 24 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. 2025

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:

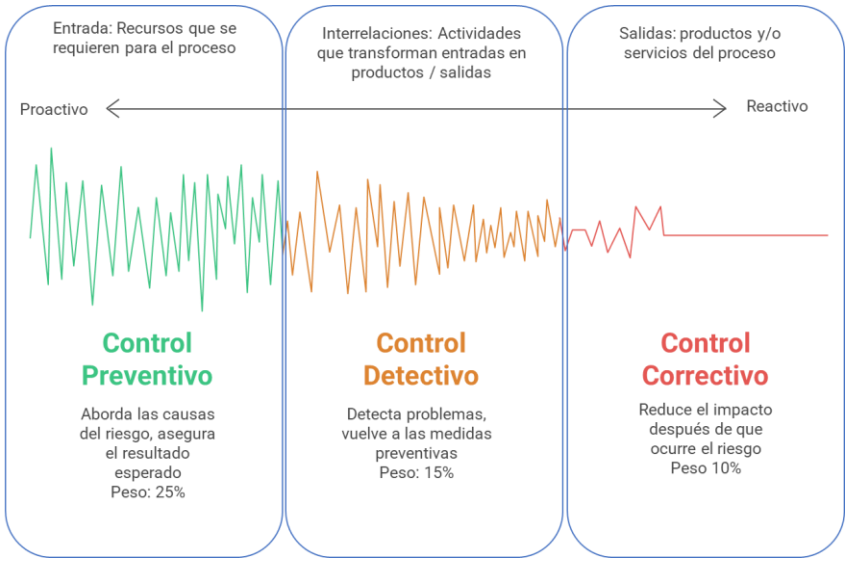
I. En caso de que el control haya sido efectivo, se notificará dentro del monitoreo realizado por la primera línea de defensa de acuerdo con lo establecido en las estrategias para la administración del riesgo
II. En caso de que el control no haya sido efectivo, dentro del seguimiento a los controles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

4. Análisis y evaluación de los controles

4.1 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 25 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. 2025.

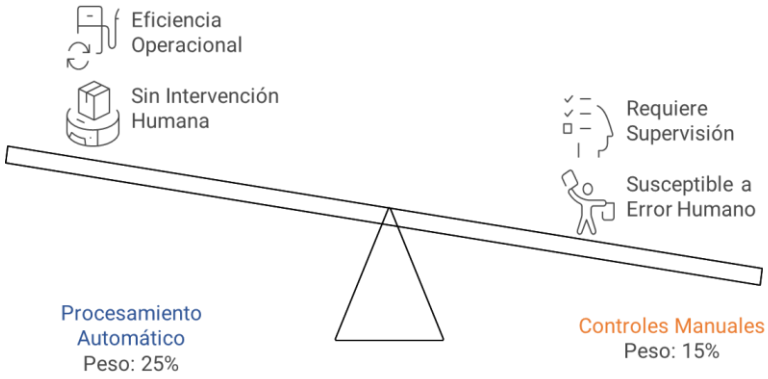
De acuerdo con el anterior esquema en el ciclo de un proceso, tenemos las siguientes tipologías de controles:

- ✓ **Control preventivo:** accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado, estos deberán tener en su redacción verbos como: Verificar, Validar, Conciliar, Comparar, Revisar, Cotejar, Detectar, Autorizar, Parametrizar (cuando son controles automáticos), entre otros que involucren acciones similares.
- ✓ **Control detectivo:** accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- ✓ **Control correctivo:** accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Se debe tener en cuenta que los controles que se contemplan en esta tipología usualmente tienen que ver con pólizas de seguro, copias de seguridad (backup), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializado, los cuales se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización pero no

pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad. En consecuencia, si bien estos controles requieren en su diseño que se apliquen actividades con un enfoque preventivo, al ser activados al momento de materialización del riesgo deben ser considerados como controles correctivos no preventivos, este tipo de controles deberán tener en su redacción verbos como: Corregir, Ajustar, Subsanar, Recuperar, Reprocesar, entre otros que involucren acciones similares

Adicionalmente se cuentan con los siguientes atributos y sus pesos:

Ilustración 26 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. 2025

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).

Tabla 10 Atributos informativos de los controles de riesgos

Característica de la Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación

Característica de la Eficiencia		Descripción
		por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional, 2025

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.

4.2 Controles asociados a la seguridad de la información

Los controles podrán elegirse los enlistados en la NTC ISO 27001:2022 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.

Tabla 11 Controles seguridad de la información

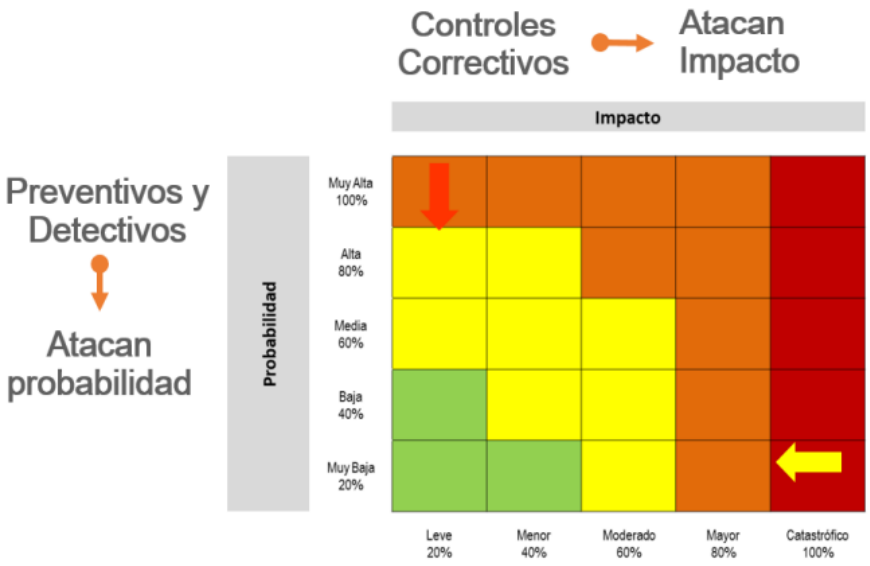
Dominio / Grupo de control	Descripción general
Controles Organizacionales	Establecen el marco de gobierno de la seguridad de la información en la organización, incluyendo políticas, roles y responsabilidades, gestión de riesgos, cumplimiento normativo y relación con terceros.
Controles de Personas	Se enfocan en la gestión del talento humano, asegurando que los colaboradores comprendan sus responsabilidades en seguridad de la información, mediante procesos como selección, capacitación, concientización y manejo de incidentes relacionados con personas.
Controles Físicos	Protegen las instalaciones, equipos e infraestructura física contra accesos no autorizados, daños o interferencias, mediante controles de acceso físico, seguridad perimetral y protección ambiental.
Controles Tecnológicos	Incluyen medidas técnicas para proteger los sistemas de información, redes y datos, como control de accesos, cifrado, gestión de vulnerabilidades, monitoreo, seguridad en redes y protección contra amenazas cibernéticas.

Fuente: ISO/IEC 27001:2022

5. 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 27 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, 2025

6. Apetito, Tolerancia y Administración Institucional del Riesgo

6.1 Apetito y Tolerancia al Riesgo

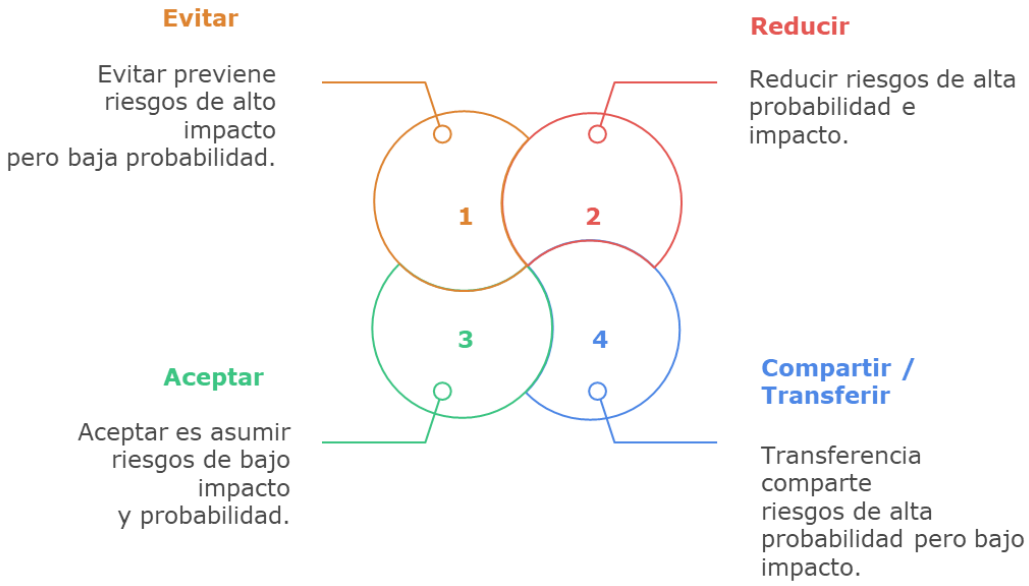
La administración del riesgo en el Ideam se fundamenta en la definición del **apetito** y la **tolerancia al riesgo**, entendidos como criterios institucionales que orientan la toma de decisiones frente a la exposición al riesgo y permiten establecer el nivel de incertidumbre que la Entidad está dispuesta a asumir para el cumplimiento de sus objetivos estratégicos y misionales.

El **apetito al riesgo** representa el nivel de riesgo que el Instituto está dispuesto a aceptar como parte del desarrollo normal de sus actividades, siempre que no comprometa el cumplimiento de la misión institucional, la generación de valor público, la integridad, la continuidad de la operación científica y técnica, el cumplimiento normativo, la seguridad de la información o la confianza de los grupos de valor.

Por su parte, la **tolerancia al riesgo** corresponde al límite máximo aceptable de desviación respecto al apetito definido. Cuando dicho límite es superado, la administración del riesgo exige la adopción de medidas adicionales de tratamiento, seguimiento y escalamiento, con el propósito de evitar la materialización de riesgos que puedan afectar significativamente el desempeño institucional.

Con el fin de facilitar la toma de decisiones y estandarizar el tratamiento de los riesgos pueden ejecutarse acciones que estén enfocadas en: reducir, evitar o compartir / transferir, su análisis se genera a partir del riesgo residual.

Ilustración 28 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. 2025

El IDEAM adopta una metodología de administración basada en niveles de exposición representados mediante un esquema de semaforización institucional, el cual se desarrolla a continuación:

6.2 Metodología Institucional para la Administración del Riesgo mediante Niveles de Exposición

La valoración del riesgo residual determinará el nivel de exposición institucional y las acciones de gestión que deberán implementar las líneas de defensa (Política De Administración Integral del Riesgo), de acuerdo con el siguiente esquema.

Tabla 12 valoración del riesgo residual y acciones de gestión

Nivel	Estado	Criterio	Administración
🟢 Bajo (Verde)	Dentro del apetito	Riesgo aceptable	Se acepta el riesgo y se mantiene el monitoreo periódico.
🟡 Moderado (Amarillo)	Cercano al límite de tolerancia	Riesgo controlable	Deben implementarse acciones de tratamiento para disminuir la probabilidad o el impacto del riesgo.
🟠 Alto (Naranja)	Supera la tolerancia	Riesgo alto	Requiere intervención prioritaria, monitoreo mensual mediante KRI y seguimiento por la Alta Dirección.
🔴 Extremo (Rojo)	Muy por encima de la tolerancia	Riesgo crítico	Requiere intervención inmediata, monitoreo mensual mediante KRI y análisis obligatorio por el Comité Institucional de Coordinación de Control Interno (CICCI).

Fuente: propia

6.3 Administración de los Riesgos según el Nivel de Exposición

6.3.1 Riesgos en Nivel Bajo

Los riesgos clasificados en nivel bajo (verde) corresponden a aquellos cuya exposición residual se encuentra dentro del apetito definido por la Entidad y cuya probabilidad e impacto son considerados aceptables para el desarrollo normal de las actividades institucionales.

Para estos riesgos:

- Se aceptará el nivel de exposición residual.
- Se mantendrán los controles implementados.
- El seguimiento se realizará conforme a la periodicidad establecida para el proceso.
- No será obligatorio implementar nuevos planes de tratamiento, salvo que el comportamiento del riesgo evidencie cambios significativos.
- La primera línea de defensa garantizará el mantenimiento de la eficacia de los controles.

6.3.2 Riesgos en Nivel Moderado

Los riesgos clasificados en nivel moderado (amarillo) indican que la exposición institucional se aproxima al límite de tolerancia definido por el Ideam.

Aunque estos riesgos aún se encuentran dentro de un nivel administrable, requieren la implementación de medidas preventivas que permitan evitar su incremento y reducir la posibilidad de materialización.

Para estos riesgos deberá:

- Elaborarse un plan de tratamiento orientado a reducir la probabilidad o el impacto del riesgo.
- Definir responsables, actividades, recursos y fechas de cumplimiento.
- Verificar periódicamente la eficacia de las acciones implementadas.
- Reportar el avance durante el seguimiento ordinario del proceso.
- Actualizar la valoración del riesgo una vez implementadas las acciones.
- El propósito de estas acciones es retornar el riesgo a niveles aceptables dentro del apetito institucional.

6.3.3 Riesgos en Nivel Alto

Los riesgos clasificados en nivel alto (naranja) corresponden a aquellos cuya exposición supera la tolerancia institucional y representan una amenaza significativa para el cumplimiento de los objetivos estratégicos, la operación institucional o la prestación de los servicios.

Estos riesgos requieren una gestión prioritaria y un seguimiento permanente por parte de las diferentes líneas de defensa.

Para estos riesgos será obligatorio:

- Formular un plan de tratamiento con acciones específicas de mitigación.
- Definir responsables de alto nivel para la ejecución de las acciones.
- Establecer Indicadores Clave de Riesgo (KRI) que permitan monitorear el comportamiento del riesgo y la eficacia de las medidas implementadas.
- Realizar seguimiento mensual a dichos indicadores.
- Informar periódicamente al Comité Institucional de Coordinación de Control Interno (CICCI), con el fin de evaluar la efectividad de las acciones implementadas y definir decisiones institucionales cuando se evidencie incremento del riesgo o incumplimiento de los planes de tratamiento.

6.3.4 Riesgos en Nivel Extremo

Los riesgos clasificados en nivel extremo (rojo) representan una exposición crítica para el Instituto y exceden ampliamente la tolerancia definida por la Alta Dirección.

Corresponden a riesgos cuya materialización puede comprometer de manera significativa el cumplimiento de la misión institucional, la continuidad de la operación, la seguridad de la información, la integridad pública, el patrimonio institucional, el cumplimiento legal o la confianza ciudadana.

Estos riesgos tendrán el mayor nivel de atención institucional.

Para su administración será obligatorio:

- Diseñar e implementar de manera inmediata un plan de tratamiento. Asignar responsables con capacidad de decisión sobre la gestión del riesgo.
- Definir y monitorear mensualmente Indicadores Clave de Riesgo (KRI).
- Evaluar mensualmente la eficacia de los controles implementados.
- Someter el análisis del riesgo al Comité Institucional de Coordinación de Control Interno (CICCI), el cual evaluará la evolución del riesgo, la suficiencia de las acciones implementadas y determinará las decisiones institucionales necesarias para reducir la exposición, reasignar recursos, fortalecer controles o definir nuevas estrategias de tratamiento.
- Mantener el seguimiento hasta que el riesgo retorne a un nivel de exposición igual o inferior al nivel amarillo.

7. 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 integridad pública: En el caso de materializarse un riesgo de integridad pública 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.

Riesgos ambientales: En caso de materializarse un riesgo ambiental, la entidad deberá implementar de manera inmediata las acciones de respuesta definidas en los instrumentos establecidos para la atención de incidentes y emergencias ambientales, con el propósito de controlar la situación, minimizar los impactos sobre el medio ambiente, proteger a las personas y dar cumplimiento a los requisitos legales y demás obligaciones aplicables.

Para la atención de estos eventos se deberá actuar conforme a los siguientes documentos del Sistema Integrado de Gestión:

- **SGI-PN003 – Plan de Contingencias para Residuos Peligrosos**, el cual establece los lineamientos para la atención de incidentes relacionados con derrames, fugas, almacenamiento, manipulación y transporte de

residuos peligrosos, con el fin de controlar la emergencia y prevenir la contaminación ambiental.

- **SGI-PN004 – Plan de Emergencias Ambientales (PREA)**, que define los procedimientos, responsabilidades y acciones para la preparación, respuesta y recuperación ante emergencias ambientales que puedan afectar los recursos naturales, las instalaciones, las personas o las comunidades, garantizando una atención oportuna y eficaz.

Una vez controlada la situación, el responsable del proceso deberá realizar el reporte del evento, evaluar la magnitud del impacto ambiental generado, identificar las causas que dieron origen a la materialización del riesgo, implementar las acciones correctivas y de mejora que correspondan y verificar su eficacia de acuerdo con el procedimiento SGI-P004 procedimiento de planes de mejoramiento, con el fin de evitar la recurrencia del evento y fortalecer los controles establecidos dentro del Sistema Integrado de Gestión.

8. Indicadores Clave de Riesgo (KRI)

Teniendo en cuenta la alineación estratégica de la gestión del riesgo y el Modelo Integrado de Planeación y Gestión (MIPG), el cual a través de la Dimensión 7 despliega los componentes de evaluación del riesgo y actividades de control en articulación con el esquema de líneas, se precisa que dicho esquema atiende de manera íntegra la gestión del riesgo al interior de la entidad, comprometiendo todos los niveles de la organización, al definir los niveles de autoridad y responsabilidad en la aplicación de controles como eje para materializar el seguimiento y monitoreo a los riesgos que enfrenta la entidad, por lo que, se hace relevante definir adecuados mecanismos para la medición del riesgo como una herramienta estratégica que permite establecer la efectividad de los controles, validar el cumplimiento de metas, analizar comportamientos y tendencias, así como identificar posibles desviaciones que puedan afectar la gestión institucional.

En este contexto, los Indicadores Clave de Riesgo (Key Risk Indicators – KRI por sus siglas en inglés), surgen como una herramienta fundamental para la toma de decisiones informadas de cara a la mitigación de riesgos, por lo que a continuación se precisan sus bases conceptuales y orientaciones técnicas para su diseño que dependerá de las características y complejidad de cada entidad.

8.1 Tipologías de Indicadores para el seguimiento

Con el propósito de definir de forma adecuada los Indicadores Clave de Riesgo, es necesario enmarcarlos desde el despliegue de la plataforma estratégica de la entidad, la cual parte de la misión, visión y valores fundamentales, base para la formulación de los objetivos estratégicos, los cuales a su vez, no solamente orientan la planeación institucional, sino que también, permiten tener un despliegue hacia los objetivos de los procesos y se constituyen en la base para la identificación y formulación de Indicadores Clave de Desempeño (Key Performance Indicators – KPI), que hacen posible medir su cumplimiento. Estos indicadores estarán referidos a aquellos que se diseñan para medir el cumplimiento misional, desde lo más estratégico hasta lo más operativo. Al respecto la Guía para la construcción y análisis de indicadores de gestión, señala lo siguiente:

Los indicadores se diseñan desde el proceso de planeación y permiten que durante las demás etapas de la gestión se verifique el cumplimiento de objetivos y metas, así como el alcance de los resultados propuestos e introducir ajustes a los planes de acción, metas o actividades. (Función Pública, 2018, p.12).

La misma guía, define los tipos de evaluación y los indicadores asociados, con una visión estratégica y el correspondiente despliegue hacia los procesos, programas y proyectos que desarrolla la entidad para su cumplimiento misional, tal como se observa en la ilustración 29.

Ilustración 29 Definición del tipo de evaluación e indicador asociado

Fuente: Departamento Administrativo de la Función Pública, 2018

En este sentido, de acuerdo con la estructura propuesta en la figura 29 se observa la forma como se vinculan los Indicadores Clave de Riesgo articulados con los Indicadores Clave de Proceso.

Ilustración 30 Articulación indicadores clave de riesgos y de los indicadores de proceso

Fuente: Adaptado documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

Se precisa entonces que, los Indicadores Clave de Riesgo (Key Risk Indicators-KRI), de acuerdo con el documento Desarrollo de Indicadores Clave de Riesgo para Fortalecer la Gestión de Riesgos Organizacional, emitido por el Committee of Sponsoring Organizations of the Treadway Commission (COSO), corresponden a:

> "(…) métricas utilizadas por las organizaciones para proporcionar una señal temprana de exposiciones al riesgo, cada vez mayores en diversas áreas de la organización. (…) estos indicadores proporcionan información oportuna sobre riesgos emergentes y potenciales que pueden tener impacto sobre el logro de los objetivos de la organización, así como las medidas en las cuales diferentes eventos o puntos desencadenantes, pueden indicar problemas que se desarrollan internamente dentro de las operaciones de la organización o los riesgos potenciales relacionados con eventos externos, esto quiere decir que pueden ofrecer información

> valiosa para la administración y la junta directiva de cada organización para tomar las medidas correctivas y preventivas para mitigar los riesgos y velar por el cumplimiento de los objetivos establecidos. (Citado por PricewaterhouseCoopers International, 2020, p.3).

Por lo tanto, estos indicadores tienen una función principal que es monitorear los riesgos clave que podrían afectar el cumplimiento de los objetivos y metas establecidos durante las diversas etapas de la gestión institucional. Así mismo, son fundamentales para realizar ajustes en la operación cuando sea necesario, lo que permite asegurar que los riesgos sean gestionados de forma adecuada y las decisiones se tomen a tiempo para mitigar cualquier desviación o amenaza.

8.2 Alcance de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI)

De acuerdo con la articulación explicada en el punto anterior, a continuación, se precisan los alcances en la aplicación de los Indicadores Clave de Proceso (KPI) y los Indicadores Clave de Riesgo (KRI), ya que, si bien tienen diferencias, resultan complementarios en su análisis. En la tabla 11 se analizan las características de cada uno.

Tabla 13 Alcance de Indicadores clave de proceso e indicadores clave de riesgo

Indicadores Clave de Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
Permiten medir periódicamente el desempeño general de la entidad y sus principales unidades operativas.	Complementan el seguimiento a los resultados de la entidad.
Se definen tomando como referencia las metas establecidas, por procesos, unidades u operaciones clave.	Proporcionan una señal temprana y oportuna de una exposición al riesgo en diversas áreas de la entidad.
Mide el rendimiento pasado, proporcionando información sobre qué tan bien se están logrando los objetivos estratégicos y operativos.	Proporcionan información útil sobre los riesgos emergentes y potenciales que pueden impactar en los objetivos estratégicos de la organización.
Ofrecen información sobre aquellos aspectos críticos de la operación que	Ayudan a identificar y anticipar problemas que se pueden presentar

Indicadores Clave de Proceso (KPI)	Indicadores Clave de Riesgo (KRI)
requieren mayores recursos y atención.	interna o externamente, así como oportunidades futuras.
Permiten medir los resultados que se obtienen de la ejecución de los programas, planes y proyectos, en los diferentes momentos o etapas de su desarrollo.	Permiten realizar un monitoreo constante y mitigar los posibles eventos de riesgo que se presenten al aplicar medidas oportunas para disminuir su impacto.
Permiten mejorar la planificación, entender con mayor precisión las oportunidades de mejora de determinados procesos y analizar el desempeño de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad.	Facilitan el proceso de generación de informes y el escalamiento de los riesgos.

Fuente: Adaptado documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

8.3 Lineamientos generales para el establecimiento de Indicadores clave de riesgo (KRI)

Para lograr una adecuada comprensión de esta tipología de indicadores, es importante retomar la definición general ya citada en el punto anterior, donde el COSO precisa que se trata de "métricas utilizadas por las organizaciones para proporcionar una señal temprana de exposiciones al riesgo". Este mismo comité a través de la estructura para el modelo COSO-ERM señala sobre estos indicadores:

> "(…) se utilizan para predecir la ocurrencia de un riesgo, generalmente son de carácter cuantitativo, pero también pueden ser cualitativos. Los indicadores clave se comunican a los niveles de la entidad que están en mejor posición para gestionar el riesgo emergente cuando sea necesario. Deberían comunicarse junto con los indicadores clave de desempeño (KPI´s) para demostrar la interrelación entre el riesgo y el desempeño. Los indicadores clave facilitan un enfoque proactivo de la gestión del desempeño. (IIA Global, PricewaterhouseCoopers, COSO-ERM. 2017, p.107)

Por su parte, la Universidad Internacional de La Rioja (2024) explica que:

> "(…) los indicadores claves de riesgo (KRI), son métricas diseñadas con el propósito de identificar y monitorear posibles amenazas que puedan afectar el cumplimiento de los objetivos de una organización. Implementarlos facilita una gestión proactiva de los riesgos, ya que proporciona información valiosa sobre tendencias o patrones que podrían indicar la aparición de problemas. Al monitorear estos indicadores, las empresas pueden ajustar su estrategia de mitigación de riesgos o de procesos, a fin de minimizar posibles impactos adversos. Para ello, es vital que las métricas estén alineadas con los objetivos y contextos de cada organización".

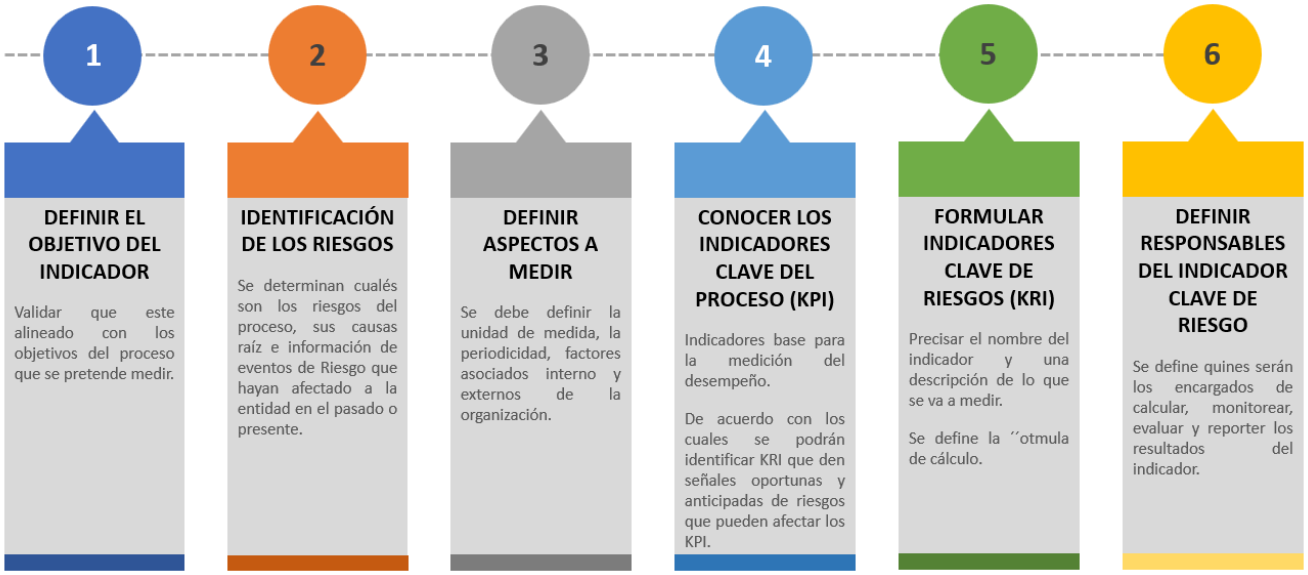
Atendiendo estas conceptualizaciones, se puede establecer que los Indicadores Clave de Riesgos (KRI), son métricas diseñadas con el fin de identificar, estimar y monitorear la ocurrencia y severidad de eventos y posibles amenazas que puedan llegar a afectar el cumplimiento de los objetivos institucionales en los diferentes niveles, por lo que se constituyen en la herramienta para el seguimiento y monitoreo de los riesgos, ya que pueden entregar señales de alerta temprana, así como detectar tendencias o cambios en los niveles de riesgo, lo que facilita que se incorporen acciones correctivas y preventivas para minimizar sus impactos frente a posibles materializaciones.

Los Indicadores Clave de Riesgos (KRI), hacen referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No necesariamente indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe analizar.

Estos indicadores permiten registrar la ocurrencia de un evento que se asocia a un riesgo identificado previamente, lo cual permite llevar un registro de eventos y evaluar a través de su tendencia la efectividad de los controles que se disponen para mitigarlos.

Para la definición y construcción de los Indicadores Clave de Riesgos (KRI), se proponen los siguientes pasos que se despliegan en la ilustración 31:

Ilustración 31 Pasos para la construcción de indicadores Clave de Riesgos (KRI)



Fuente: Adaptado de Documento PricewaterhouseCoopers International Limited, Indicadores clave de riesgo y Pirani Risk, Guía Práctica Indicadores Clave de Riesgo por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2025.

Para el desarrollo de los anteriores pasos se debe tener en cuenta:

i. **Definir el objetivo del indicador**, el cual debe estar alineado con los objetivos del proceso, plan, programa o proyecto que se pretende medir.
ii. **Identificar los riesgos**, en este paso se determinan cuáles son los riesgos del proceso, plan, programa o proyecto, sus causas raíz e información de eventos de riesgo que hayan afectado a la entidad en el pasado o presente, se deberán priorizar aquellos que en su residualidad estén en alto o extremo.

Sobre la gestión de eventos, se trata de un riesgo materializado, donde se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente. Algunas fuentes para establecer una base histórica de eventos pueden ser: i) mesas de ayuda; ii) PQRD (peticiones, quejas, reclamos, denuncias); iii) Oficina jurídica; iv) Líneas internas y externas de denuncia.

iii. **Definir los aspectos a medir**, para lo cual se deben establecer la unidad de medida, la periodicidad, los factores internos o externos de la entidad y especialmente, que se pretende medir.

iv. **Conocer los Indicadores Clave de Proceso (KPI),** teniendo en cuenta que estos son la base de medición del desempeño del proceso, programa o proyecto.

v. **Formular el Indicador Clave de Riesgo (KRI)**, se debe precisar como mínimo lo siguiente:

   a. El nombre del indicador,
   b. una descripción de lo que se va a medir,
   c. la fórmula de cálculo,
   d. La fuente de información para el cálculo del indicador, por ejemplo: sistemas internos, reportes de auditoría, bases de datos internas y/o externas u otras fuentes,
   e. frecuencia de medición y seguimiento y;
   f. umbrales de alerta.

Algunos ejemplos de indicadores se presentan en la tabla 14:

Tabla 14 Ejemplo Indicadores Clave Riesgo (KRI)

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible

Fuente: Adaptado del listado de indicadores y métricas (www.riesgoscero.com) por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

En este punto se deben establecer los umbrales de alerta, ya que no todos los cambios en los KRI requieren acción inmediata, por lo que, es fundamental que el líder del proceso, plan, programa o proyecto defina los umbrales de alerta que señalen cuándo un KRI alcanza un nivel que requiere atención, lo que permite a la entidad priorizar las áreas que necesitan intervención inmediata y distinguirlas de aquellas situaciones donde los riesgos están bajo control.

Para este efecto, para cada KRI se debe definir una semaforización que permita distinguir entre valores aceptables, riesgosos o críticos, así:

✓ Valor Bajo (Verde): Valor mínimo deseado

✓ Valor Moderado (Amarillo): Valor que indica riesgo potencial

✓ Valor Alto (Rojo): Valor crítico o inaceptable

Estos valores dependerán del proceso, plan, programa o proyecto que se esté analizando y de sus indicadores clave de desempeño.

Ahora bien, es fundamental comprender que el resultado del cálculo del KRI se relaciona directamente con el apetito al riesgo, y debe ser analizado de cara a la declaración de apetito de la entidad bajo las siguientes consideraciones.

i) **Valor del KRI dentro del apetito al riesgo**: Significa que la operación de la entidad, y por ende el riesgo se sigue moviendo dentro delo que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.

ii) **Valor del KRI que excede el apetito al riesgo**: Significa que el riesgo ha superado el umbral que la entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. En este caso se deben tomar acciones correctivas o de mitigación para llevar el riesgo de nuevo hacia un rango tolerable.

iii) **Valor del KRI se acerca al umbral de alerta definido**: Revela que el riesgo se ha ido aumentando y que podría salir del umbral de alerta si continua así.

Ejemplo

Supongamos que el apetito de riesgo de una entidad ha fijado que el número de quejas de los usuarios puede ser de hasta 10 quejas al mes sin que eso genere una intervención.

Si el KRI revela que se han presentado 8 quejas, significa que la entidad está muy cerca del umbral (10), aumentando el riesgo de que el asunto se pueda salir de control.

Si el KRI llega a 12 quejas, significa que el riesgo ha excedido el apetito y será necesario implementar medidas correctivas.

Finalmente, se debe considerar que, si bien los umbrales de alerta en primera instancia son definidos por los líderes de los procesos, planes, programas y proyectos, dado que son ellos quienes conocen en mayor detalle su operatividad, estos deberán ser analizados y aprobados por la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno.

vi. **Definir los responsables del Indicador Clave de Riesgos (KRI)**, será necesario definir quiénes serán los encargados de calcular, monitorear, evaluar y reportar los resultados del indicador.

Algunas recomendaciones a tener en cuenta para identificar y formular los Indicadores Clave de Riesgo (KRI) para una mayor efectividad se señalan a continuación:

✓ Relevancia: Deben estar alineados con los riesgos críticos para la entidad.

✓ Cuantificables: Es fundamental que los Indicadores Clave de Riesgo (KRI) puedan ser medidos de manera objetiva.

✓ Predictivos: Un buen Indicador Clave de Riesgo (KRI) debería ser capaz de predecir o bien detectar posibles problemas antes de que ocurran.

✓ Comparables: Los Indicadores Clave de Riesgo (KRI) deben permitir la comparación a lo largo del tiempo para identificar tendencias.

En cuanto a las limitaciones que pueden presentarse en el diseño de estos indicadores se tienen las siguientes:

✓ Un Indicador Clave de Riesgo (KRI) no sustituye la comprensión integral del contexto de la entidad, es decir, se requiere un conocimiento del entorno y las características de la entidad para diseñar y medir estos indicadores.

✓ Si la fuente de información (interna o externa) no es confiable porque esta desactualizada, es errada y/o no posee un histórico de datos podría ocasionar Indicadores Clave de Riesgo (KRI) ineficientes.

✓ Si presentan fallas en el establecimiento de los umbrales de los Indicadores Clave de Riesgo (KRI) puede generar que no se ajusten las estrategias de la entidad de manera proactiva y puede disminuir la probabilidad del cumplimiento de las metas y objetivos institucionales.

8.4 Comunicación y reporte KRI en el marco del esquema de líneas de aseguramiento

En concordancia con lo dispuesto en el Esquema de Líneas de Aseguramiento, eje articulador para la política de control interno, Dimensión 7 de MIPG, para los Indicadores Clave de Riesgo (KRI) por su enfoque preventivo, y que se articulan a los Indicadores Clave de Proceso (KPI), se requiere para cada uno de los roles identificados un trabajo conjunto para contribuir colectivamente a la generación de alertas tempranas, con el fin de fortalecer la gestión del riesgo y evitar su materialización.

La definición de los roles y las responsabilidades se encuentran en la política integral para la administración integral del riesgo del Ideam

9. Monitoreo del riesgo

De acuerdo con la cultura del autocontrol cada responsable de proceso debe realizar el respectivo monitoreo a los riesgos de gestión, de integridad pública, 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, integridad pública, 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 15:

Tabla 15 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 BIMENSUAL
	Alta	Se realiza seguimiento a los controles con periodicidad MENSUAL, a partir de los indicadores clave de riesgo
	Extrema	Se realiza seguimiento a los controles con periodicidad MENSUAL, a partir de los indicadores clave de riesgo
Riesgos de Integridad pública	Todos los riesgos de integridad pública serán monitoreados de acuerdo a la zona del riesgo en la que se encuentran para el caso de MODERADO de manera BIMENSUAL. Aquellos en zona ALTA Y EXTREMA de manera MENSUAL (a partir de los indicadores clave de riesgo)	

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 integral 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 integral identificados 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, integridad pública 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.

10. Actualización al mapa de riesgos

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/ función de cumplimiento 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.

11. Implementación

Para la implementación de la presente guía, 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.

11.1 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 16 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.

Rol en el aplicativo o herramienta tecnológica definido desde la OAP	Responsabilidad
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 2026

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 guía.

Cultura Organizacional y Madurez del Sistema Integral de Gestión del Riesgo

La consolidación del Sistema Integral de Gestión del Riesgo del IDEAM requiere fortalecer no solamente la aplicación de metodologías para identificar, valorar y tratar riesgos, sino también desarrollar una cultura organizacional basada en la prevención, el autocontrol, la toma de decisiones informadas y la mejora continua.

En este contexto, el Instituto adopta el **Modelo de Madurez del Sistema Integral de Gestión del Riesgo** como un instrumento de autodiagnóstico institucional que permite evaluar periódicamente el nivel de desarrollo de la gestión del riesgo, determinar las brechas existentes frente a las mejores prácticas internacionales y establecer las acciones necesarias para fortalecer la capacidad institucional.

La evaluación de la madurez constituye un mecanismo de aseguramiento que permite verificar la evolución del Sistema Integral de Gestión del Riesgo y medir el grado de apropiación de la Política de Administración Integral del Riesgo en todos los niveles organizacionales.

La evaluación de madurez tiene como propósito:

- Evaluar el grado de implementación del Sistema Integral de Gestión del Riesgo.
- Medir la evolución de la cultura institucional del riesgo.
- Identificar fortalezas y oportunidades de mejora.
- Determinar las brechas existentes frente al modelo de referencia.
- Priorizar acciones de fortalecimiento institucional.
- Orientar la actualización de la Política y de la Guía de Administración Integral del Riesgo.
- Apoyar la toma de decisiones por parte del Comité Institucional de Coordinación de Control Interno (CICCI).

Dimensiones del Modelo de Madurez

La evaluación de madurez se desarrollará sobre cinco dimensiones estratégicas, las cuales representan los elementos esenciales para garantizar la efectividad del Sistema Integral de Gestión del Riesgo.

a. Gobierno y Cultura

Esta dimensión evalúa el grado de liderazgo institucional, el compromiso de la Alta Dirección y la apropiación de la gestión del riesgo en todos los niveles de la organización.

Su propósito es determinar si la gestión del riesgo hace parte de la cultura institucional y cuenta con estructuras de gobierno claramente definidas.

Comprende los siguientes principios:

- Supervisión del riesgo por el Comité Institucional de Coordinación de Control Interno.
- Definición de estructuras operativas para la gestión del riesgo.
- Desarrollo de una cultura organizacional orientada a la prevención.
- Compromiso con los valores del servicio público.
- Desarrollo y fortalecimiento de las competencias del talento humano.

b. Estrategia y Definición de Objetivos

Evalúa el grado de integración entre la gestión del riesgo y el direccionamiento estratégico institucional.

Su finalidad es verificar que la administración del riesgo contribuya al cumplimiento de la misión, los objetivos estratégicos y la generación de valor público.

Comprende los principios relacionados con:

- Análisis permanente del contexto institucional.
- Definición y comunicación del apetito al riesgo.
- Evaluación de estrategias institucionales.
- Integración del riesgo en la planeación.

c. Desempeño

Evalúa la capacidad institucional para gestionar los riesgos durante la ejecución de los procesos.

Analiza la aplicación efectiva de la metodología institucional para:

- Identificación de riesgos.
- Evaluación del riesgo inherente.
- Diseño y evaluación de controles.
- Valoración del riesgo residual.

- Implementación de acciones de tratamiento.

d. Análisis y Monitorización

Esta dimensión determina la capacidad institucional para evaluar permanentemente el comportamiento del riesgo y la eficacia del Sistema de Gestión Integral del Riesgo.

Comprende aspectos relacionados con:

- Monitoreo de cambios del contexto.
- Identificación de riesgos emergentes.
- Seguimiento a la evolución del riesgo.
- Evaluación del desempeño institucional.
- Implementación de Indicadores Clave de Riesgo (KRI).
- Revisión y mejora continua de la gestión del riesgo.

e. Información, Comunicación y Reporte

Evalúa la capacidad institucional para generar información confiable sobre la gestión del riesgo y facilitar la toma de decisiones en todos los niveles organizacionales.

Esta dimensión comprende:

- Gestión de la información.
- Uso de herramientas tecnológicas.
- Comunicación institucional del riesgo.
- Reportes para la Alta Dirección.
- Reportes de riesgos materializados.
- Reportes sobre cultura del riesgo.

Evaluación de la Madurez

La Oficina Asesora de Planeación, como segunda línea de defensa, realizará anualmente la aplicación de la herramienta de diagnóstico, consolidando la información suministrada por las diferentes dependencias y verificando la evidencia que soporte cada una de las calificaciones asignadas.

Los resultados deberán presentarse al Comité Institucional de Coordinación de Control Interno (CICCI), el cual evaluará el estado de madurez del Sistema Integral de Gestión del Riesgo, analizará las brechas identificadas y definirá las

acciones institucionales necesarias para fortalecer los componentes que presenten menores niveles de desarrollo, entre las acciones de mejora podrán incluir, entre otras:

- Actualización de políticas, metodologías y procedimientos.
- Fortalecimiento del esquema de gobernanza del riesgo.
- Desarrollo de estrategias para consolidar la cultura de autocontrol.
- Capacitación y entrenamiento de servidores públicos y contratistas.
- Implementación de indicadores clave de riesgo (KRI).
- Fortalecimiento de herramientas tecnológicas para la gestión del riesgo.
- Revisión y ajuste de controles.
- Incorporación de riesgos emergentes y riesgos transversales.
- Mejoramiento de los mecanismos de seguimiento y reporte

Así mismo se deberá realizar seguimiento periódico, con el fin de avanzar en el cierre de brechas.

Mejora Continua del Sistema Integral de Gestión del Riesgo

El Modelo de Madurez constituye el principal mecanismo de evaluación estratégica del Sistema Integral de Gestión del Riesgo del Ideam y opera bajo el modelo de operación por procesos. Los resultados del autodiagnóstico alimentan la revisión de la Política de Administración Integral del Riesgo, la actualización de la presente Guía, la formulación de planes institucionales y la priorización de recursos para consolidar una cultura preventiva.

Documentos relacionados en el SGI

- Política para la Administración Integral del Riesgo
- 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
- Guía para la administración integral del riesgo.
- Programa de Transparencia y Ética Pública
- Manual de Debida Diligencia
- Política de Integridad
- Manual de políticas complementarias de seguridad y privacidad de la información

- Plan de continuidad del Negocio
- Plan institucional SGSST
- Procedimiento de conflicto de interés
- Política de imparcialidad
- Guía de identificación de aspectos e impactos ambientales

Bibliografía

- Guía Para Para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2025
- Instituto de Auditores Internos/ PricewaterhouseCoopers. PwC. COSO Committee of Sponsoring Organizations of the Treadway Commission. (2017). Gestión del riesgo empresarial, integrando estrategia y desempeño.
- Fundación Latinoamericana de Auditores Internos FLAI. The Institute of Internal Auditors, Inc. Perspectivas y percepciones globales, Gobernanza, riesgo y control. (2023).
- Universidad del Rosario. (2020). Curso Riesgo Operativo.
- Organización Internacional de Normalización (ISO). (2018). ISO 31000. Gestión del riesgo. Directrices.
- Instituto de Auditores Internos de España. (2013). Fábrica de Pensamiento. Definición e implantación de apetito del riesgo. https://auditoresinternos.es/centro-de-conocimiento/fabrica-de-pensamiento/
- Instituto de Auditores Internos de España. (2021). Fábrica de Pensamiento. Auditoría Interna y gestión de riesgos. https://auditoresinternos.es/centro-de-conocimiento/fabrica-de-pensamiento/
- Superintendencia Financiera de Colombia. Apetito del riesgo, guía externa. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1072547
- Departamento Administrativo de la Función Pública. (2020). Guía para la gestión por procesos en el marco de MIPG.
- PwC. (2020). Indicadores claves de riesgo. https://www.pwc.com/ve/es/publicaciones/assets/PublicacionesNew/Boletines/Indicadores%20claves%20de%20riesgo-oct2020.pdf
- COSO (2010). Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks. Research Commissioned by the Committee of Sponsoring Organizations of the Treadway Commission.
- Armijo, Mariela. (2011). Planificación estratégica e indicadores de desempeño en el sector público. CEPAL. 2011. https://repositorio.cepal.org/server/api/core/bitstreams/dfa8d5f1-7315-4f10-9824-8fa5b005cc1b/content

- Universidad Internacional de La Rioja. (2024). Indicadores clave para la gestión del riesgo en las organizaciones. UNIR Ecuador. https://ecuador.unir.net/actualidad-unir/indicadores-clave-riesgo/
- Delfiner, M., & Pailhé, C. (2008). Técnicas cualitativas para la gestión del riesgo operacional. BCRA.
- Contraloría General de la República. (2023). Cartilla para el fortalecimiento de hallazgos con incidencia fiscal 2023. Contraloría Delegada para Responsabilidad Fiscal, Intervención Judicial y Cobro Coactivo. https://www.ascontrol.org/sites/default/files/estandar/2023/08/Cartilla%20para%20el%20Fortalecimiento%20de%20Hallazgos%20con%20Incidencia%20Fiscal%202023.pdf
- OCDE (2020), Manual de la OCDE sobre Integridad Pública, OECD Publishing, Paris, https://doi.org/10.1787/8a2fac21-es
- Organización Internacional de Normalización (ISO). (2025). ISO 37001. Sistemas de gestión antisoborno. Requisitos con orientación para su uso.

Control de cambios

Versión	Fecha	Descripción
01	22/07/2026	Se separa de la metodología para la identificación, evaluación y valoración de riesgos, de la Se realiza la actualización de la política. Adicionalmente se actualiza: Capítulo de Metodología para la administración integral del riesgo: contexto, riesgos emergentes, riesgos de integridad, riesgos ambientales, riesgos transversales. Se define apetito y tolerancia del riesgo armonizada con la política de

		administración integral del riesgo. Se incluye indicadores clave de riesgo. Se incluye capitulo de: cultura organizaciones y madurez del Sistema integral del riesgo.