Agencia Nacional Digital

POLITICA DE GESTION INTEGRAL DEL RIESGO

BOGOTÁ, OCTUBRE DE 2026

Agencia Nacional Digital

Contenido

1. OBJETIVO 5
1.1 Objetivos Específicos 5
2. ALCANCE 5
3. DEFINICIONES 6
4. DOCUMENTOS REFERENCIA 9
5. POLÍTICA GESTIÓN INTEGRAL DEL RIESGO 10
6. ESTRUCTURA ORGÁNICA 11
7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO EN LA AND 14
7.1 Marco de referencia COSO-ERM adoptado por la Agencia 15
8. GESTIÓN DE RIESGOS 16
8.1 Lineamientos Riesgos relacionados con posibles actos de corrupción – Riesgos para la Integridad Pública (SIGRIP) 16
8.2 Lineamientos Riesgos de Seguridad de la información 17
8.3 Apetito del Riesgo (Niveles de Aceptación del Riesgo) 18
8.3.1 Determinación de la Capacidad del Riesgo: 18
8.3.2 Determinación del Apetito del Riesgo: 19
8.3.3 Tolerancia del Riesgo: 19
8.4 Niveles para la Calificación del Impacto 20
8.4.1 Niveles para la Calificación de la Probabilidad 22
8.5 Estrategias para combatir el riesgo 22
8.6 Identificación y descripción del riesgo 23
8.7 Clasificación del riesgo por factor 24
8.8 Diseño y documentación de controles 26
8.9 Valoración de controles y determinación del riesgo residual 27
8.10 Lineamientos Riesgos Fiscales 28
8.11 Consolidación, actualización e inactivación de riesgos 28
Para crear, modificar o inactivar riesgos o controles se requiere aprobación del líder del proceso o gerente del proyecto y del responsable del equipo con funciones de Planeación. Se consideran vigentes únicamente los riesgos y controles contenidos en la versión más reciente de la Agencia. 28
8.12 Indicadores clave de riesgo (KRI) e indicadores de control 28
9. ESQUEMA DE LAS LÍNEAS DE DEFENSA 29
10. ROLES Y RESPONSABILIDADES 30

10.1 Línea estratégica 30
10.2 Primera línea de defensa 32
10.3 Segunda línea de defensa 33
10.4 Tercera línea de defensa 34
11. Seguimiento y Registro de riesgos materializados 35
12. MONITOREO 36
13. COMUNICACIÓN 37
14. CUMPLIMIENTO 38
15. VIGENCIA DE LA POLÍTICA 38

INTRODUCCIÓN

La gestión del riesgo constituye un elemento fundamental para la toma de decisiones, el fortalecimiento institucional y el logro de los objetivos estratégicos de la Corporación Agencia Nacional de Gobierno Digital o Agencia Nacional Digital (AND). Su aplicación permite identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos que puedan afectar el cumplimiento de la misión institucional, la prestación de los servicios, la ejecución de los proyectos, la gestión de la seguridad de la información y la generación de valor público.

En este sentido, la AND adopta la Gestión Integral del Riesgo como una práctica transversal a todos los procesos, proyectos y actividades de la entidad, promoviendo la prevención, la anticipación y la mejora continua como mecanismos para fortalecer el desempeño institucional, la transparencia, el control y la capacidad de respuesta frente a eventos internos y externos que puedan impactar el logro de los objetivos.
La presente Política de Gestión Integral del Riesgo establece los lineamientos generales para la administración de los riesgos institucionales y se fundamenta en los siguientes principios:

- **Integración al direccionamiento estratégico:** La gestión del riesgo hace parte de la planeación, la gestión institucional y la toma de decisiones en todos los niveles de la organización.
- **Cultura de prevención:** Todos los colaboradores son responsables de identificar y gestionar oportunamente los riesgos asociados a sus actividades y procesos.
- **Mejora continua:** La gestión del riesgo se evalúa y fortalece permanentemente con el fin de responder a los cambios del entorno y a las necesidades institucionales.
- **Responsabilidad compartida:** La gestión del riesgo es una responsabilidad de todos los niveles de la entidad, de acuerdo con las funciones y competencias asignadas.
- **Toma de decisiones basada en riesgos:** La definición de estrategias, planes, proyectos e iniciativas institucionales deberá considerar los riesgos y oportunidades que puedan afectar el logro de los objetivos.

A partir de estos principios, la Agencia orienta la gestión integral del riesgo como una herramienta de apoyo para la generación de valor, la protección de los recursos institucionales y el fortalecimiento de la gobernanza organizacional.

1. OBJETIVO

Establecer los lineamientos que le permitan a AND proteger todos sus procesos de los potenciales riesgos asociados, así como establecer los mecanismos necesarios para evitar, reducir, compartir, transferir y/o mitigar los riesgos inherentes a su quehacer institucional y que pudieran afectar a las personas, las instalaciones, los bienes y los equipos de la entidad, y los objetivos institucionales, en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo Estándar de Control Interno (MECI) y la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del Departamento Administrativo de la Función Pública (DAFP).

1.1 Objetivos Específicos

- Proporcionar a la administración lineamientos para un aseguramiento razonable, orientado al cumplimiento de sus objetivos
- Establecer los roles y responsabilidades de las líneas de defensa de la entidad
- Establecer los criterios de identificación, análisis, valoración, tratamiento, monitoreo y comunicación aplicables a todas las tipologías de riesgo gestionadas por la Agencia.
- Definir los niveles de aceptación del riesgo (apetito, tolerancia y capacidad) y las medidas de respuesta asociadas a cada nivel de severidad.
- Brindar criterios técnicos para el diseño, documentación y valoración de controles que reduzcan la probabilidad de ocurrencia y/o el impacto de los riesgos identificados.
- Definir el tratamiento aplicable a los riesgos materializados, incluidos los eventos materializados no identificados previamente.
- Promover una cultura de prevención, integridad y transparencia orientada a la protección de los recursos públicos y a la generación de valor público.

2. ALCANCE

La presente política aplica para la gestión de riesgos, incluyendo aquellos que se pueden derivar de los procesos definidos, igualmente se consideran los que pueden afectar la prestación de los servicios o cualquier otra actividad de la AND. Cobija a todas las dependencias, procesos estratégicos, misionales, de apoyo y de evaluación, proyectos, planes y programas, así como a servidores, colaboradores, contratistas y terceros que ejecuten actividades en nombre de la Agencia.

Comprende las siguientes tipologías de riesgo: riesgos de gestión, riesgos para la integridad pública (incluidos los riesgos de corrupción y los asociados a LA/FT/FP), riesgos de seguridad de la información y riesgos fiscales. Su aplicación es transversal al Sistema Integrado de Gestión de la AND y se articula con las demás políticas institucionales.

3. DEFINICIONES

Con el propósito de facilitar la comprensión de la Política se deben tener en cuenta las siguientes definiciones:

a. **Administración del Riesgo:** un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

b. **Apetito de Riesgo:** es el nivel de riesgo que la Agencia puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

c. **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

d. **Gestión del Riesgo:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

e. **Identificación del Riesgo:** etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.

f. **Impacto:** consecuencias o efectos que pueden ocasionar a la organización la materialización del riesgo.

g. **Matriz de Riesgo:** documento en el cual se plasma la representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

h. **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.

i. **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

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

k. **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. A partir de la Versión 7 de la Guía de Función Pública, esta categoría se gestiona dentro de la tipología de **riesgos para la integridad pública**, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).

l. **Riesgos de gestión:** posibilidad de que un evento potencial afecte el cumplimiento de los objetivos de los procesos de la organización, sus definiciones estratégicas, o su operación. Estos riesgos pueden ser de carácter judicial, contractual, financiero, administrativo, imagen, asociados a la prestación de servicios, fiscales, contables y presupuestales.

m. **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).

n. **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).

o. **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.

p. **Riesgos para la Integridad Pública:** posibilidad de que se presenten conductas o situaciones que afecten la integridad en el ejercicio de la función pública, tales como corrupción, soborno, fraude, conflicto de intereses y lavado de activos, financiación del terrorismo y de la proliferación de armas de destrucción masiva (LA/FT/FP).

q. **SIGRIP:** Sistema de Gestión de Riesgos para la Integridad Pública, definido en la Versión 7 de la Guía de Función Pública y articulado con el componente programático de la Estrategia Institucional para la Lucha Contra la Corrupción y con el Programa de Transparencia y Ética Pública.

r. **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo; no constituyen la causa principal o base para que este se presente.

s. **Causa raíz:** causa principal o básica; corresponde a las razones por las cuales se puede presentar el riesgo y es la base para la definición de controles.

t. **Riesgo inherente:** nivel de riesgo propio de la actividad, sin considerar la aplicación de controles.

u. **Riesgo residual:** nivel de riesgo resultante después de aplicar y valorar los controles existentes.

v. **Control:** medida que modifica el riesgo, actuando sobre sus causas o sobre sus consecuencias. Puede ser preventivo, detectivo o correctivo, y de ejecución manual o automática.

w. **Punto de riesgo:** actividad crítica dentro de la cadena de valor del proceso en la cual se materializa la exposición al riesgo.

x. **Severidad:** resultado de combinar la probabilidad de ocurrencia y el impacto del riesgo; se representa en el mapa de calor.

y. **Indicador clave de riesgo (KRI):** métrica que permite anticipar variaciones en el nivel de exposición al riesgo o alertar sobre el deterioro de los controles.

z. **Nivel de madurez de la gestión del riesgo:** grado de desarrollo de las capacidades institucionales para gestionar el riesgo, evaluado sobre los componentes y principios del marco COSO-ERM adoptados por la Versión 7 de la Guía de Función Pública.

4. DOCUMENTOS REFERENCIA

- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6. Función Pública, diciembre 2022.

Marco normativo y técnico aplicable:

- Ley 87 de 1993 – Normas para el ejercicio del control interno en las entidades del Estado.
- Ley 1474 de 2011 – Estatuto Anticorrupción (artículo 73, mapa de riesgos de corrupción).
- Ley 2195 de 2022 – Medidas de transparencia y prevención de la corrupción, y programas de transparencia y ética pública.
- Decreto 1499 de 2017 – Modelo Integrado de Planeación y Gestión – MIPG.
- Decreto 648 de 2017 – Esquema de líneas de defensa y rol de las oficinas de control interno.
- Decreto 1083 de 2015 (Único Reglamentario del Sector de Función Pública) y sus modificaciones.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. Departamento Administrativo de la Función Pública, septiembre de 2025.
- Anexo Técnico del Programa de Transparencia y Ética Pública – Secretaría de Transparencia de la Presidencia de la República.
- Guía No. 7 de Gestión de Riesgos de Seguridad Digital – Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- NTC-ISO 31000:2018 – Gestión del riesgo. Directrices.
- NTC-ISO/IEC 27001:2022 e ISO/IEC 27005 – Gestión de la seguridad de la información y gestión de riesgos de seguridad de la información.
- DE.MN.01 Manual del SIG AND y Resolución 019 de 2021 "Por la cual se adopta el SIG AND".

5. POLÍTICA GESTIÓN INTEGRAL DEL RIESGO

La AND, se compromete a fortalecer la cultura de prevención, por medio de una adecuada gestión de riesgos, dirigiendo sus esfuerzos hacia el establecimiento de los mecanismos necesarios para evitar, reducir/mitigar, compartir/transferir y/o asumir los riesgos relacionados con el desarrollo de todos sus procesos y que pudieran afectar negativamente a las personas, las instalaciones y/o los bienes de la entidad; para tal efecto realizará la identificación, análisis, valoración e intervención de los riesgos inherentes al quehacer institucional, contribuyendo de esta forma al logro de los objetivos y la misión de la entidad.

La Agencia, por medio de la alta dirección asigna los recursos necesarios para lograr esta gestión del riesgo, propiciando los espacios que sean necesarios para que sus colaboradores participen de forma activa en todas las actividades relacionadas con el tema, lo anterior aplicando lo establecido en la presente Política y en el procedimiento de administración de riesgos.

En desarrollo de esta política, la Agencia Nacional Digital se compromete específicamente a:

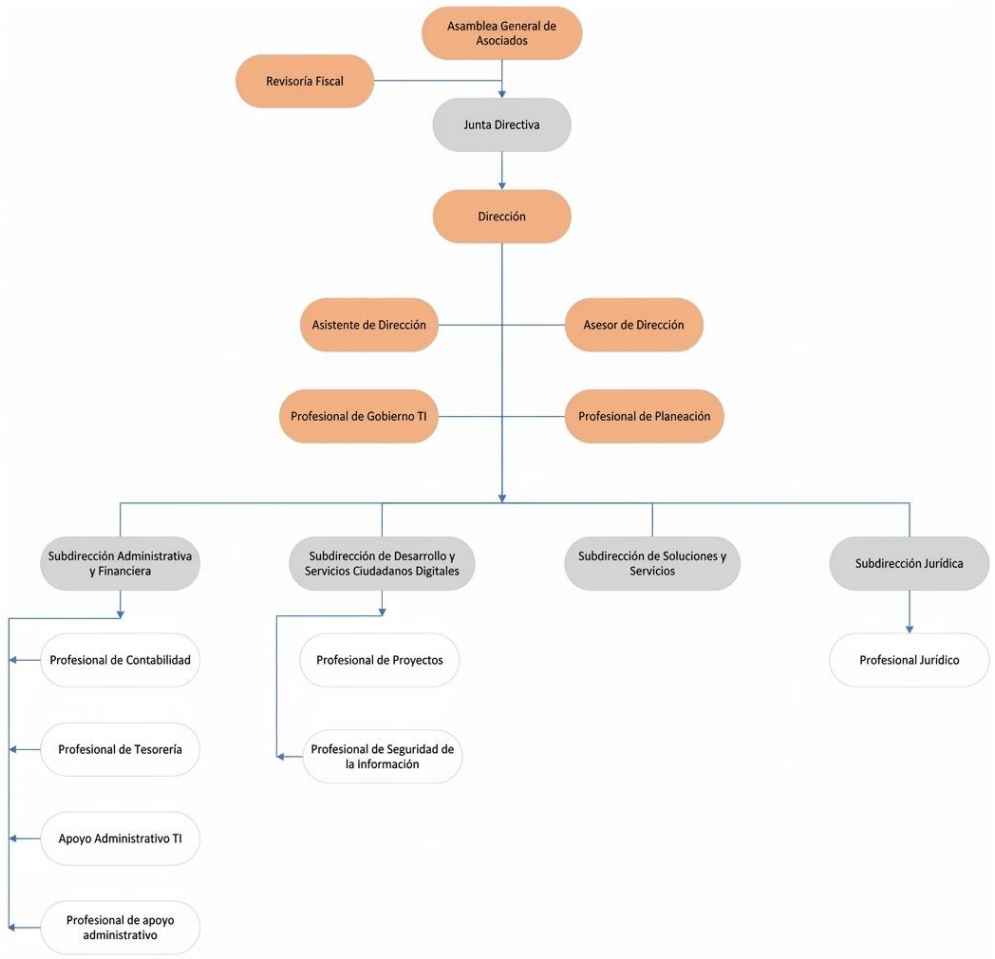
- Gestionar de manera integral las tipologías de riesgo
- Mantener los niveles de exposición dentro del apetito y la tolerancia definidos por la alta dirección, formulando acciones de tratamiento para todo riesgo que los supere.
- Diseñar controles documentados, con responsable, periodicidad, forma de ejecución y evidencia verificable, evaluando periódicamente su eficacia y eficiencia.
- Aplicar cero tolerancia frente a los riesgos para la integridad pública: estos riesgos no se aceptan ni se transfieren, y siempre requieren acciones de tratamiento.
- Reportar de manera oportuna la materialización de riesgos, incluidos los eventos no identificados previamente, y adoptar planes de mejoramiento derivados del análisis de causa raíz.
- Evaluar anualmente el nivel de madurez de la gestión integral del riesgo y ejecutar acciones de cierre de brechas.

Así mismo, los riesgos positivos que se identifican se entienden como oportunidades de mejora y se potencializan para ser aprovechados y mejorar los resultados de nuestra gestión institucional. Las oportunidades se gestionan en el marco del Sistema

Integrado de Gestión y no se registran en el mapa de riesgos, el cual se reserva a eventos de efecto adverso, conforme a la metodología de Función Pública.

6. ESTRUCTURA ORGÁNICA

Figura 1. Estructura organizacional AND



Fuente: www.and.gov.co

PLATAFORMA ESTRATÉGICA

Misión

Impulsar la transformación digital del Estado mediante la articulación, prestación y evolución de los Servicios Ciudadanos Digitales y el desarrollo de soluciones de ciencia, tecnología e innovación aplicada, para fortalecer la gestión pública, facilitar el acceso de ciudadanos y empresas a la administración pública y contribuir a un Estado más eficiente, transparente, participativo y sostenible.

Visión

En 2030, la AND será reconocida como la entidad referente que moviliza la transformación digital del Estado colombiano, ampliando la cobertura y el impacto de los Servicios Ciudadanos Digitales y desarrollando soluciones integrales de ciencia, tecnología e innovación aplicada que fortalezcan la gestión pública, impulsen la innovación pública y mejoren la vida de los ciudadanos.

Objetivos estratégicos

1. Ampliar la cobertura en los procesos de articulación y prestación de los SCD en las entidades públicas y privadas.

2. Integrar soluciones y servicios enfocados en Ciencia, Tecnología e Innovación que aporten a la transformación digital del estado colombiano.

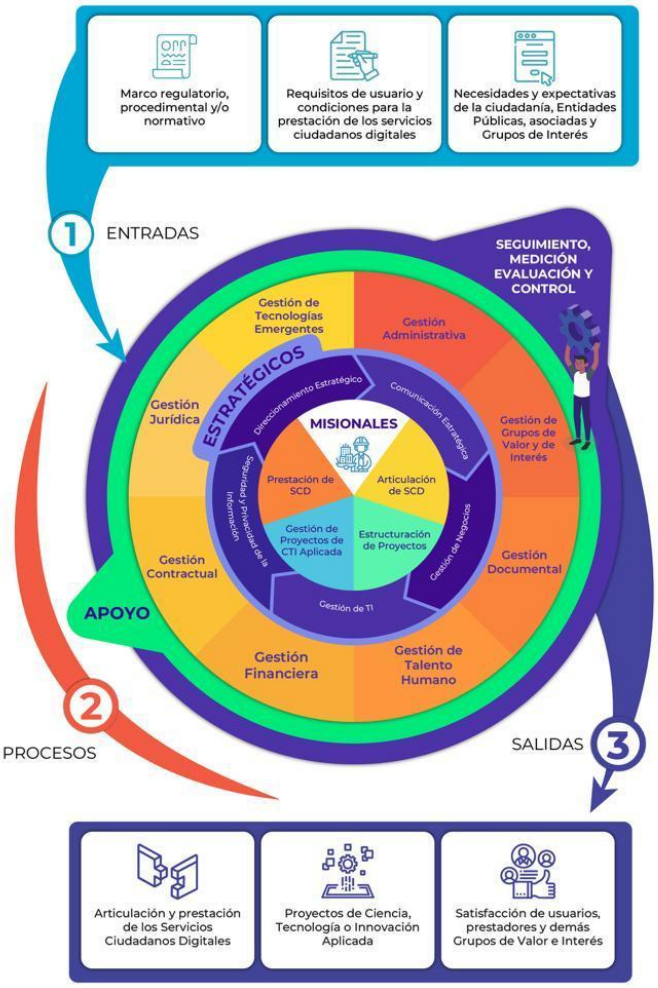
3. Consolidar el modelo de gestión y negocio que permita la autosostenibilidad y posicionamiento en el mercado.

4. Potenciar la AND como una entidad eficiente a través de un equipo humano competente para el logro de los objetivos organizacionales

Mapa de procesos institucional

Figura 2. Mapa de procesos





Fuente: www.and.gov.co

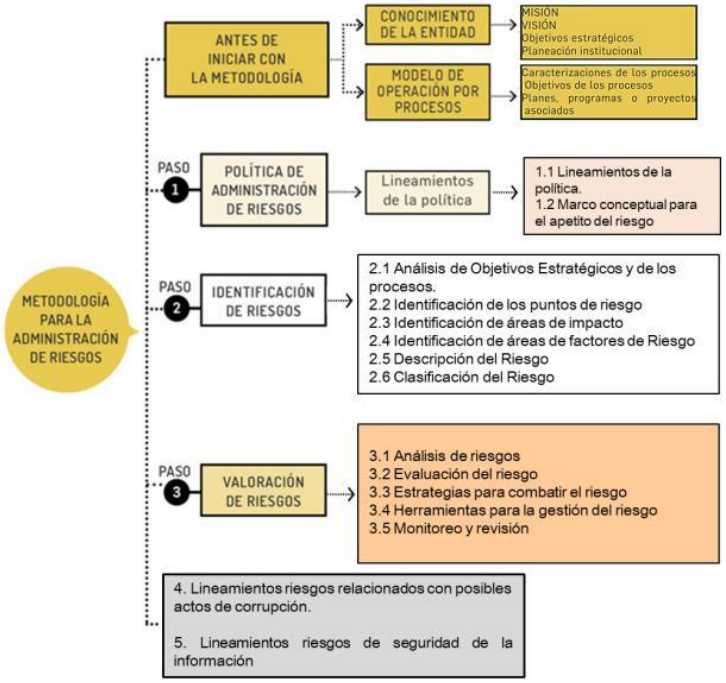
7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO EN LA AND

La AND implementa las etapas de identificación y valoración de los riesgos, teniendo como referencia la Guía para la Administración del riesgo y el diseño de controles en entidades públicas –Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del Departamento Administrativo de la Función Pública.

Así mismo, la AND aplica su metodología de administración de riesgos en sus diferentes proyectos de desarrollo, reconociendo la importancia de controlar de forma organizada la ejecución de las actividades de control en sus proyectos, como también contar con un establecimiento adecuado de los riesgos que identifica, con el fin de prevenir sus materializaciones; enfocándose en el tratamiento efectivo de las causas que generan estos riesgos. Cabe mencionar, que la presente política sirve como base para elaborar los diferentes planes de riesgos en los proyectos de Desarrollo.

A continuación, se aprecia la figura 3, que muestra de manera general la metodología aplicada en la Agencia.

Figura 3. Metodología para la gestión del Riesgo en la AND



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, Departamento Administrativo de la Función Pública, 2025.

Antes de iniciar con la metodología, es necesario contar con la información que permita llevar a cabo una contextualización de la organización, partiendo del conocimiento de la Entidad en cuanto a su misión, visión, objetivos estratégicos y su planeación institucional. En la Agencia Nacional Digital este contexto se encuentra plasmado en el Plan Estratégico Institucional el cual rige el quehacer de la Entidad.

De igual manera es fundamental que la Entidad cuente con un Modelo de Operación por Procesos en el marco del cual se evidencie la estructura para la gestión en la entidad a partir de los procesos identificados y en los cuales se pueda llevar a cabo la gestión de riesgos. En la Agencia Nacional Digital, dicho modelo se encuentra descrito en el DE.MN.01 Manual del SIG AND y en la Resolución 019 de 2021 "Por la cual se adopta el SIG AND".

En este contexto, la Agencia Nacional Digital cuenta con la intranet como la herramienta por medio de la cual se encuentra la información de los diferentes procesos de la Entidad, los cuales cuentan con cartas descriptivas o caracterizaciones en las cuales se establecen los objetivos de los procesos y se enmarcan los planes o proyectos que genera la Agencia. En el caso de los proyectos de Ciencia Tecnología e Innovación aplicada, así como de Prestación y Articulación de Servicios Ciudadanos Digitales, es importante adicionar el análisis del contexto de acuerdo con la particularidad de cada proyecto (Ej. Entidad para la que se desarrolla el proyecto, población objetivo del proyecto, etc.)

7.1 Marco de referencia COSO-ERM adoptado por la Agencia

La Agencia adopta la estructura de gestión integral del riesgo descrita en la Versión 7 de la Guía de Función Pública, basada en el marco COSO-ERM (2017), integrada por cinco componentes:

- **Gobierno y cultura:** base de los demás componentes; define lineamientos, roles, responsabilidades y la cultura frente al riesgo. En la AND se materializa a través del Comité Institucional de Coordinación de Control Interno y del esquema de líneas de defensa descrito en el capítulo 9.
- **Estrategia y establecimiento de objetivos:** articula la gestión del riesgo con el Plan Estratégico Institucional, el análisis de contexto y la definición del apetito del riesgo.
- **Desempeño:** identificación, análisis, priorización y respuesta a los riesgos que pueden afectar el logro de los objetivos.
- **Revisión y monitorización:** evaluación de cambios significativos, revisión del desempeño de la gestión del riesgo y búsqueda de la mejora.

- **Información, comunicación y reporte:** obtención y divulgación continua de información sobre riesgo, cultura y desempeño, teniendo en cuenta el Plan Estratégico y la Política de Comunicación vigentes de la Agencia.

8. GESTIÓN DE RIESGOS

La Agencia Nacional Digital utiliza como principal referente para la gestión de riesgos la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del Departamento Administrativo de la Función Pública. De igual manera se tendrá en cuenta el anexo A de la ISO/IEC 27001:para la identificación de controles de los riesgos de seguridad de la información, así como la Guía No. 7 de MinTIC.

Las desviaciones que se puedan presentar en el seguimiento a los procesos, indicadores, cronogramas y demás herramientas que sean utilizadas en la Agencia para la gestión de los riesgos, deberán ser tratadas a través de planes de mejoramiento, los cuales deberán ser notificados por medio de correo electrónico a Control Interno, quien realizará el seguimiento correspondiente a las actividades propuestas.

8.1 Lineamientos Riesgos relacionados con posibles actos de corrupción – Riesgos para la Integridad Pública (SIGRIP)

La Versión 7 de la Guía de Función Pública sustituye el capítulo de riesgos de corrupción por el **Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP)**, articulado con el componente programático de la Estrategia Institucional para la Lucha Contra la Corrupción y con el Anexo Técnico del Programa de Transparencia y Ética Pública. En consecuencia, la Agencia Nacional Digital gestiona estos riesgos conforme a los siguientes lineamientos:

- Amenazas a considerar: soborno (entrante y saliente), fraude, conflicto de intereses, corrupción y LA/FT/FP.
- El análisis de contexto para esta tipología debe incluir: planta y estructura de la entidad y la delegación de autoridad o poder decisorio discrecional; grupos de valor y contrapartes; jurisdicciones o territorios donde opera; naturaleza, escala y complejidad de procesos, servicios y trámites; segmentación de contratos y principales proveedores; entidades que ejercen control sobre la AND y sobre las que la AND ejerce control; e interacciones con otras ramas del poder público y con particulares.

- Estos riesgos se identifican y describen con la misma estructura general (evento no deseado, causa inmediata, causa raíz e impacto) definida en el numeral 8.6.
- Cero tolerancia: los riesgos para la integridad pública no se aceptan ni se transfieren. Todo riesgo de esta tipología requiere acciones de tratamiento, con independencia de su nivel residual.
- Monitoreo cuatrimestral por la primera línea de defensa y seguimiento cuatrimestral por la Oficina de Control Interno, con publicación de resultados conforme a la Ley 1474 de 2011 y la Ley 2195 de 2022.
- Toda materialización debe ser reportada de manera inmediata al equipo con funciones de Planeación y al Comité Institucional de Coordinación de Control Interno, y activar los canales de denuncia dispuestos por la Agencia.

El mapa de riesgos para la integridad pública hace parte integral del mapa institucional de riesgos y se articula con el Programa de Transparencia y Ética Pública de la Agencia.

8.2 Lineamientos Riesgos de Seguridad de la información

Los riesgos de seguridad de la información serán identificados, valorados y tratados de acuerdo con la metodología descrita en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del DAFP, complementada con la Guía No. 7 de MinTIC y las normas ISO/IEC 27001:2022 e ISO/IEC 27005.

La identificación parte del inventario de activos de información de cada proceso y de su clasificación según criticidad, confidencialidad, integridad y disponibilidad. Para esta tipología, además de la afectación económica y reputacional, se evalúa la **afectación operativa** derivada de la indisponibilidad, pérdida de integridad o divulgación no autorizada de la información.

Nota: Al finalizar la evaluación de los riesgos identificados y la aceptación del riesgo deberá quedar formalmente aprobada y documentada por el líder del proceso o responsable del activo de información, esto con el fin de establecer responsabilidad en la gestión de los riesgos de seguridad digital.

8.3 Apetito del Riesgo (Niveles de Aceptación del Riesgo)

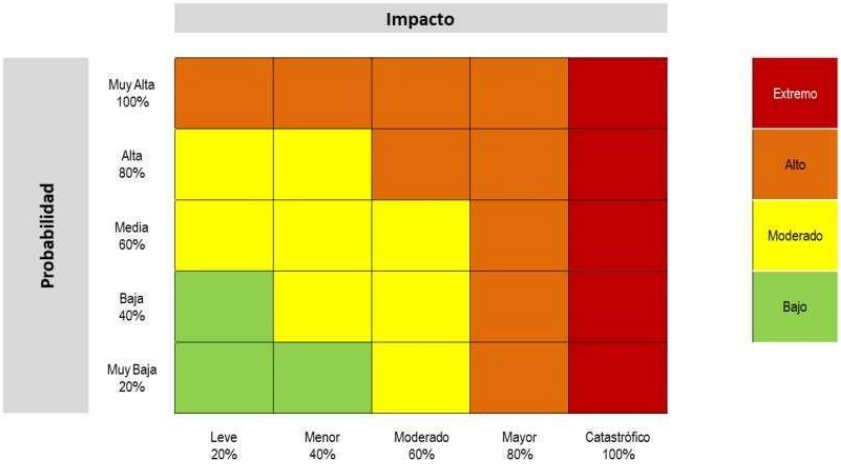
El apetito del riesgo o el nivel del riesgo que la Agencia puede aceptar está dado por los objetivos de la Agencia, el marco legal y disposiciones de la alta dirección. En este sentido a continuación se determina la capacidad del riesgo, el apetito del riesgo y la tolerancia del riesgo para la AND:

8.3.1 Determinación de la Capacidad del 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 que no sería posible el logro de los objetivos de la entidad.

En este contexto, la escala que resulta de combinar la probabilidad y el impacto en la valoración de los riesgos genera los niveles de riesgo, estos son: extremo, alto, moderado y bajo, tal como se muestra en la siguiente figura:

Figura 4. Matriz de calor – Niveles de severidad del riesgo



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

En este marco, la Agencia Nacional Digital define que el valor máximo de la escala del nivel del riesgo que puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos, es el nivel del riesgo extremo, siendo este su capacidad de riesgo.

8.3.2 Determinación del Apetito del Riesgo:

El valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad. Equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

En este contexto, la Agencia Nacional Digital define que el nivel de riesgo que la entidad puede aceptar es el nivel **Moderado** para todas las tipologías de riesgo.

8.3.3 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. Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

En este marco, la Agencia Nacional Digital define que la tolerancia del riesgo se establece de manera diferenciada por tipología, conforme a la siguiente tabla:

Tabla 1. Niveles de aceptación del riesgo por tipología

Tipología de riesgo	Apetito	Tolerancia	Capacidad
Riesgos de gestión	Bajo	Moderado a Alto	Extremo
Riesgos de seguridad de la información	Bajo	Moderado	Alto
Riesgos fiscales	Bajo	Moderado	Alto
Riesgos para la integridad pública (SIGRIP)	Bajo	No aplica – cero tolerancia	No aplica

Fuente: Elaboración propia con base en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

La Alta Dirección considera que el nivel de riesgo extremo es el valor máximo que podrá ser resistido por la entidad manteniendo la capacidad de cumplir con sus objetivos. Todo riesgo cuyo nivel residual supere la tolerancia definida requerirá acciones de tratamiento con responsable, fecha de implementación y fecha de seguimiento. En todo caso, para los riesgos incluidos en las matrices se deben formular acciones de tratamiento cuando el nivel residual sea superior al apetito.

Teniendo en cuenta todo lo anterior, en la siguiente tabla se definen las medidas de respuesta que se pueden ejecutar dependiendo del nivel de Riesgo:

Tabla 2. Medidas de Respuesta a Niveles de severidad del riesgo

Nivel del Riesgo	Medidas de Respuesta
Riesgo nivel Bajo	Aceptar el Riesgo
Riesgo nivel Moderado	Reducir el Riesgo
Riesgo nivel Alto	Reducir el Riesgo, Transferir el Riesgo o Evitar el Riesgo
Riesgo nivel Extremo	Reducir el Riesgo, Transferir el Riesgo o Evitar el Riesgo
Riesgos para la integridad pública (cualquier nivel)	Reducir o Evitar. No se acepta ni se transfiere; siempre requiere plan de tratamiento.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

8.4 Niveles para la Calificación del Impacto

De conformidad con la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. Función Pública, 2025, se dispone la siguiente tabla para la calificación del impacto:

Tabla 3. Calificación del Impacto de riesgos

Nivel	Descriptor	Afectación económica	Reputacional
1	Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
2	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.
3	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.
4	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.
5	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: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

Nota: cuando para un mismo riesgo se identifiquen simultáneamente afectación económica y reputacional en niveles distintos, se tomará siempre el nivel más alto. Los rangos en SMLMV serán validados anualmente frente al presupuesto anual de la Agencia, y ajustados cuando dejen de ser representativos.

8.4.1 Niveles para la Calificación de la Probabilidad

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo y está asociada a la exposición de la actividad analizada; corresponde al número de veces que se pasa por el punto de riesgo en el período de un (1) año. Para su calificación se aplica la siguiente tabla:

Tabla 4. Criterios para definir el nivel de probabilidad

Nivel	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 1 vez por año	20 %
Baja	La actividad que conlleva el riesgo se ejecuta de 2 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 de 501 a 5.000 veces por año	80 %
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año	100 %

Fuente: Adaptado de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025. Los rangos de frecuencia se ajustan al volumen operativo de la AND y deben validarse anualmente.

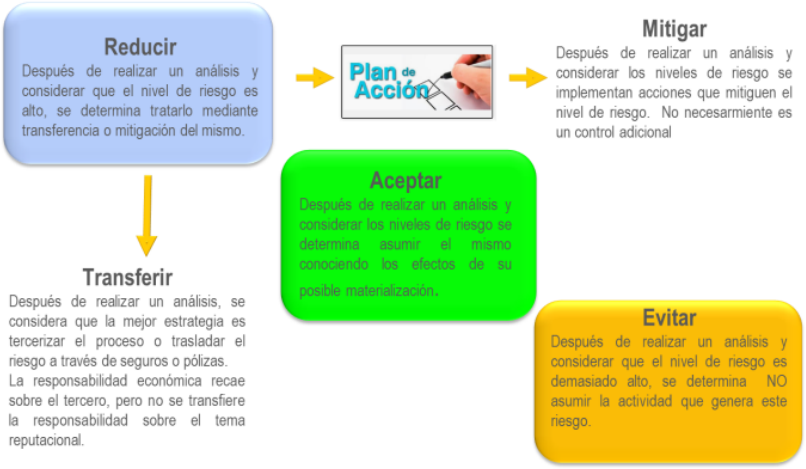
Ejemplo de aplicación: si el proceso debe publicar 8 documentos 4 veces al año, la actividad se ejecuta 8 x 4 = 32 veces al año, lo que corresponde a una probabilidad Media (60 %). Este valor es el que se registra en la matriz de riesgos.

8.5 Estrategias para combatir el riesgo

Es la decisión que se toma frente a un determinado nivel de riesgo, la cual puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente. En la siguiente ilustración se observan las tres opciones mencionadas y su

relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Ilustración 1. Estrategias para combatir el Riesgo



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.

8.6 Identificación y descripción del riesgo

La identificación del riesgo es desarrollada por el líder del proceso o gerente de proyecto (primera línea de defensa), con acompañamiento del equipo con funciones

de Planeación (segunda línea). Toma como insumos el contexto estratégico interno y externo, la caracterización del proceso y sus actividades críticas, el inventario de activos de información, el historial de hallazgos y materializaciones, y el análisis de los objetivos estratégicos y de proceso.

En su desarrollo se responden las siguientes preguntas:

- ¿Qué puede suceder? Identificar la afectación al cumplimiento del objetivo estratégico o del proceso.
- ¿Cómo puede suceder? Establecer las causas a partir de los factores determinados en el contexto.
- ¿Cuándo puede suceder? Determinar el momento del proceso en que se presenta la exposición.
- ¿Qué consecuencias tendría su materialización? Determinar los posibles efectos económicos y reputacionales.

La descripción del riesgo se estructura a partir de tres elementos: **impacto** (consecuencia económica y/o reputacional), **causa inmediata** (circunstancia más evidente sobre la cual se presenta el riesgo) y **causa raíz** (razón principal o básica, base para la definición de controles). Un mismo riesgo puede tener varias causas o subcausas.

Reglas de redacción obligatorias:

- Los riesgos no se describen como fallas ni desviaciones de los controles.
- No se describe el riesgo como la negación del control (por ejemplo, "no realizar la verificación…").
- No existen riesgos transversales; lo que puede existir son causas transversales.
- El evento debe ser específico y claro, no genérico, y expresarse en términos de qué podría pasar.

8.7 Clasificación del riesgo por factor

Los factores de riesgo son las fuentes generadoras que incrementan la probabilidad de ocurrencia del evento. No son causas directas, pero elevan el nivel de exposición. La Agencia adopta la siguiente clasificación:

Tabla 5. Factores de riesgo

Factor	Descriptores
Ejecución y administración de procesos	Estructura organizacional que afecta la capacidad institucional; falta de aplicación de los procedimientos; falta de segregación de funciones; errores de grabación o 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 contractuales, de empleo, salud o seguridad en el trabajo; falta de capacitación.
Talento humano	Fraude interno; soborno entrante y saliente; gestión inadecuada de conflicto de intereses; corrupción; hurto de activos.
Tecnología	Daño de equipos; caída de sistemas de información y aplicaciones; caída de redes; errores en hardware o software; errores en programas.
Infraestructura	Derrumbes; incendios; inundaciones; daños a activos fijos.
Evento externo	Fraude externo; suplantación de identidad; asalto a las instalaciones; atentados, vandalismo y alteraciones del orden público.
Transacción u operación (aplica para LA/FT/FP)	Contrapartes de la entidad (naturales o jurídicas); productos, bienes o servicios que oferta o requiere; canales utilizados para la operación; jurisdicciones nacionales o territoriales.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

Adicionalmente, y dada la misionalidad de la Agencia, en el análisis de contexto deberán considerarse de manera expresa los factores asociados a la transformación digital, la ciberseguridad, la dependencia de proveedores tecnológicos y de servicios en la nube, la protección de datos personales, la sostenibilidad ambiental y el relacionamiento con la ciudadanía y con las entidades usuarias de los Servicios Ciudadanos Digitales.

8.8 Diseño y documentación de controles

Las actividades de control deben atender las causas raíz y enfocarse en la gestión de los factores de riesgo y describirse con la siguiente estructura:

Tabla 6. Estructura para la descripción del control

Elemento	Descripción
Responsable	Cargo o rol que ejecuta el control, con nivel de autoridad apropiado y respetando la segregación de funciones. En controles automáticos, se identifica el responsable de su parametrización o calibración.
Objetivo del control	Verbo que identifica la acción: verificar, validar, conciliar, comparar, revisar, cotejar, detectar.
Frecuencia	Periodicidad de ejecución (permanente, por evento, diaria, mensual, trimestral, etc.), adecuada al nivel de exposición inherente.
Ejecución	Cómo se ejecuta el control, con qué fuentes de información (internas, externas o mixtas) y qué se hace ante desviaciones.
Evidencia	Fuente documental que demuestra la ejecución: formato, base de datos, lista de chequeo, acta, registro físico o electrónico.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

Según su oportunidad, los controles se clasifican en **preventivos** (actúan sobre las causas antes de la actividad originadora), **detectivos** (se activan durante la ejecución y pueden generar reprocesos) y **correctivos** (actúan después de la materialización y tienen costos implícitos). Según su forma de ejecución, son **manuales** o **automáticos**.

8.9 Valoración de controles y determinación del riesgo residual

Cada control se valora según sus atributos de eficiencia, conforme a los siguientes pesos:

Tabla 7. Atributos de eficiencia del control

Atributo	Peso	Descripción
Preventivo	25 %	Actúa sobre las causas del riesgo y asegura el resultado final esperado.
Detectivo	15 %	Detecta la ocurrencia y devuelve el proceso a los controles preventivos; puede generar reprocesos.
Correctivo	10 %	Reduce el impacto una vez materializado el riesgo; tiene costo de implementación.
Automático	25 %	Se ejecuta por un sistema o aplicativo sin intervención humana.
Manual	15 %	Es ejecutado por una persona; lleva implícito el error humano.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

Los controles preventivos desplazan el riesgo en el eje de probabilidad; los detectivos también actúan sobre la probabilidad; los correctivos desplazan el riesgo en el eje de impacto. El riesgo residual se calcula aplicando sucesivamente el valor de cada control:

$$PR = PI - (PI \times VC)$$

Donde PI es la probabilidad inherente, PR la probabilidad residual y VC la valoración del control. Cuando existe más de un control para el mismo riesgo, la probabilidad residual del primero se convierte en la probabilidad inherente del siguiente ($PR_2 = PR_1 - (PR_1 \times VC_2)$), y así sucesivamente. La misma lógica se aplica al impacto para los controles correctivos.

Adicionalmente, los controles se evalúan en su **eficacia** (grado en que el control evita la materialización del riesgo) y en su **eficiencia** (relación entre el resultado obtenido y los recursos empleados en su ejecución), conforme a los indicadores definidos en el numeral 8.12.

8.10 Lineamientos Riesgos Fiscales

La gestión preventiva del riesgo fiscal busca evitar el daño sobre los recursos públicos, los bienes o los intereses patrimoniales de naturaleza pública. Su identificación parte del historial de hallazgos con incidencia fiscal, de las observaciones de los organismos de control y de la identificación de puntos de riesgo fiscal en los procesos de planeación, contratación, ejecución presupuestal, supervisión y pagos.

La descripción del riesgo fiscal se estructura a partir de: el **evento potencial** (hecho incierto que puede ocurrir), la **causa inmediata**, la **causa raíz o potencial hecho generador** y el **efecto** (daño cuantificable sobre los recursos públicos).

8.11 Consolidación, actualización e inactivación de riesgos

Para crear, modificar o inactivar riesgos o controles se requiere aprobación del líder del proceso o gerente del proyecto y del responsable del equipo con funciones de Planeación. Se consideran vigentes únicamente los riesgos y controles contenidos en la versión más reciente de la Agencia.

La inactivación de un riesgo requiere justificación técnica y detallada del líder responsable y no procederá cuando existan recomendaciones u observaciones pendientes sobre ese riesgo o sus controles en informes de auditoría, evaluación o seguimiento. La decisión queda registrada en el informe de seguimiento de la segunda línea de defensa, garantizando su trazabilidad.

8.12 Indicadores clave de riesgo (KRI) e indicadores de control

La Agencia define indicadores que permiten anticipar variaciones en el nivel de exposición y evaluar el desempeño de los controles. Como mínimo se mantendrán los siguientes:

Tabla 8. Indicadores clave de riesgo y de control

Indicador	Descripción y periodicidad
Materialización de riesgos	Número de riesgos materializados en el período sobre el total de riesgos identificados. Semestral.
Eventos materializados no identificados	Número de eventos materializados que no estaban en el mapa de riesgos. Semestral.
Eficacia del control	Porcentaje de controles ejecutados con evidencia verificable sobre el total de controles programados. Semestral.
Eficiencia del control	Controles que operan sin generar reprocesos ni sobrecostos frente al total evaluado. Anual.
Cumplimiento de acciones de tratamiento	Acciones de tratamiento ejecutadas dentro del plazo sobre el total formuladas. Semestral.
Riesgos fuera de tolerancia	Número de riesgos con nivel residual superior a la tolerancia definida. Semestral.
Madurez de la gestión del riesgo	Resultado del autodiagnóstico de madurez frente a la meta institucional. Anual.

Fuente: Elaboración propia con base en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

9. ESQUEMA DE LAS LÍNEAS DE DEFENSA

De conformidad con lo establecido en el MIPG, se describe la siguiente metodología, en la cual se define el esquema de las líneas de defensa adoptado por la Agencia Nacional Digital:

Tabla 9. Esquema de las líneas de defensa

Nivel	Descripción
Línea Estratégica Alta Dirección, Comité de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno	Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos, tiene la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad.
1ª Línea de Defensa Medidas de control interno del día a día, ejecutadas por el equipo de trabajo, y controles de gerencia operativa ejecutados por un jefe	La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.
2ª Línea de Defensa Media y alta gerencia: jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, comités de riesgos, comité de contratación, áreas financieras y de TIC, entre otros	Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, y supervisa la implementación de prácticas de gestión de riesgo eficaces. Consolida y analiza información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
3ª Línea de Defensa Control Interno	Desarrolla los componentes de Control Interno: 1. Liderazgo Estratégico. 2. Enfoque hacia la Prevención. 3. Evaluación de la Gestión del Riesgo. 4. Relación con Entes Externos de Control. 5. Evaluación y Seguimiento.

Fuente: Elaboración propia con base en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. DAFP, 2025.

10. ROLES Y RESPONSABILIDADES

10.1 Línea estratégica

Tabla 10. Líneas estratégicas

Responsable	Responsabilidad frente al riesgo
Alta Dirección. Comité de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno	• Aprobar la Política de Gestión Integral del riesgo. • Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la Agencia y que puedan generar cambios en la estructura de los riesgos identificados y en sus actividades de control. • Realizar seguimiento y análisis periódico a los riesgos institucionales. • Revisar la exposición de la entidad a los riesgos de corrupción y fraude de acuerdo con los informes del canal de denuncias PQRSD. • Monitorear el tratamiento de las denuncias de riesgos de corrupción y fraude desde el Comité Institucional de Coordinación de Control Interno. • Realimentar en el Comité Institucional de Gestión y Desempeño los ajustes que se deban hacer frente a la gestión del riesgo. • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este. • Monitorear el cumplimiento de los estándares de conducta y la práctica de los principios y valores de los funcionarios públicos por medio del Comité Institucional de Coordinación de Control Interno.
Director(a)	• Aprobar las directrices determinadas de la Administración de Riesgos aplicables a la entidad. • Definir el marco general para la administración del riesgo. • Presentar los cambios en el Direccionamiento Estratégico y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados. • Hacer seguimiento en el Comité Institucional de Coordinación de Control Interno en la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno.

10.2 Primera línea de defensa

Tabla 11. Primera línea de defensa

Responsable	Responsabilidad frente al riesgo
Líderes de procesos / Gerentes de proyecto	• Realizar el análisis de contexto y análisis de causas, relacionados con cada mapa de riesgos que lidera. • Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlos cuando se requiera. • Realizar la evaluación del riesgo inherente y riesgo residual, aplicando las actividades de control que correspondan. • Definir, aplicar y hacer seguimiento a las actividades de control para tratar los riesgos identificados, alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso o proyecto. • Aprobar los riesgos formulados o actualizados. • Supervisar la ejecución de las actividades de control aplicadas por el equipo de trabajo en la gestión del día a día. Detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar, con base en la evaluación del diseño de actividades de control. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de las actividades de control. • Informar a Planeación o quien haga sus veces (segunda línea) sobre los riesgos materializados en los programas, planes y/o procesos a su cargo. En el caso de los proyectos de desarrollo, el Gerente debe informar al cliente en las reuniones de seguimiento programadas, y coordinar con Control Interno (tercera línea) el establecimiento del plan de mejoramiento respectivo. • Diligenciar el mapa de riesgos del proceso o proyecto liderado, el cual debe ser aprobado por la AND (en el caso de los proyectos, requiere aprobación del cliente) y mantenerlo actualizado; en caso de requerir asesoría por parte de Planeación, realizar la solicitud correspondiente. • Los líderes de Procesos, Proyectos, propietarios y responsables de Activos de Información son los encargados de realizar la gestión del Riesgo sobre dichos Activos de Información. El Oficial de Seguridad de la Información debe promover y apoyar la

Responsable	Responsabilidad frente al riesgo
	ejecución de esta actividad, basado en la metodología aprobada para tal fin.

10.3 Segunda línea de defensa

Tabla 12. Segunda línea de defensa

Responsable	Responsabilidad frente al riesgo
Persona o equipo asignado para realizar las funciones de Planeación en la AND	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional y presentar en el comité de gestión y desempeño los riesgos de mayor criticidad frente al logro de los objetivos para análisis y seguimiento. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y proyectos. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Presentar a la Línea Estratégica alertas sobre eventos y cambios en el entorno.
Profesional asignado como Oficial de seguridad de la información	Evaluar el cumplimiento de los controles asociados a las Políticas de Seguridad de la Información.
Subdirector jurídico	• Monitorear la gestión contractual y generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas. • Monitorear la gestión jurídica, generando alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas en esta materia.
Subdirector administrativo / Profesional asignado	• Hacer monitoreo a las PQRD generando alertas sobre incumplimientos, quejas en la prestación del servicio, tutelas u otras situaciones de riesgo detectadas. • Monitorear temas clave del ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral,

Responsable	Responsabilidad frente al riesgo
	código de integridad), generando alertas sobre incumplimientos, situaciones críticas que afectan el clima laboral y posibles afectaciones al código de integridad. • Monitorear el Plan Estratégico de Tecnologías de la Información - PETI.
Gerentes de proyectos	Monitorear aspectos estructurales de los temas bajo su gestión, generando alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas acorde con las materias a su cargo.

Se adiciona al equipo con funciones de Planeación: aplicar anualmente el autodiagnóstico de madurez; consolidar y reportar los indicadores del numeral 8.12; y verificar que todo ajuste al mapa institucional cuente con el acta exigida en el numeral 8.11.

10.4 Tercera línea de defensa

Tabla 13. Tercera línea de defensa

Responsable	Responsabilidad frente al riesgo
Persona o equipo asignado para realizar las funciones de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de las actividades de control establecidas en los procesos y proyectos. • Proporcionar aseguramiento objetivo en los procesos y proyectos identificados no cubiertos por la primera y segunda línea de defensa. • Acompañar de forma coordinada con el equipo de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y en el diseño de las actividades de control. • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Programa Anual de Auditoría. • Recomendar mejoras a la política y guía de administración del riesgo.

Responsable	Responsabilidad frente al riesgo
	• Comunicar a la Alta Dirección sobre posibles materializaciones de riesgos críticos en la Agencia. • Realizar acompañamiento a los Gerentes de Proyecto de desarrollo, sobre la aplicación correcta de la presente política. • Evaluar la eficacia de las actividades de control establecidas por la primera línea de defensa en los diferentes mapas de riesgo.

11. Seguimiento y Registro de riesgos materializados

El seguimiento de los riesgos identificados se realizará con base en el nivel de riesgo residual de acuerdo con las escalas descritas en la matriz de calor residual, de la siguiente manera:

Nivel de Riesgo Residual	Periodicidad de Seguimiento
Extremo	Mensual
Alto	Trimestral
Moderado	Semestral
Bajo	Anual

El seguimiento principal estará en cabeza de los líderes de procesos y el equipo de trabajo que se designe para este fin, posteriormente desde el rol de Planeación, se realizará el seguimiento de acuerdo con la periodicidad descrita en la tabla anterior, en el caso que sea necesario, se realizarán las recomendaciones necesarias en relación con el diseño y ejecución de los controles incluidos los controles que mitigan los riesgos estratégicos o institucionales.

Anualmente se revisará el mapa de riesgos completo, tomando como base las auditorías realizadas por Control Interno, los organismos de control y las notificaciones de materialización realizadas por los líderes de procesos y gerentes de proyecto, con el objetivo de actualizar el mapa de riesgos institucional conforme a los cambios presentados en cada vigencia. Adicional, en este seguimiento se realizará la

verificación de la efectividad de los controles identificados en los riesgos de los procesos y proyectos.

El reporte de los eventos de riesgos materializados será enviado mediante correo electrónico por el Líder del proceso o gerente de proyecto, al equipo asignado con funciones de Planeación, el cual debe informar la situación presentada (incluyendo el análisis de causas respectivo), fecha inicio y fin del suceso, fecha de reporte, riesgo al cual está asociado, proceso o proyecto en donde se identificó el suceso, impacto, acciones adelantadas, actividades de control relacionadas y consecuencias. Este reporte debe realizarse cuando el evento del riesgo materializado se presente, y en todo caso dentro de los tres (3) días hábiles siguientes a su conocimiento.

Partiendo del análisis de causas del evento materializado, se debe formular un plan de mejora que indique la corrección o actividades de mitigación de este.

Materialización de riesgos no identificados: cuando se presente un evento adverso que no estuviera incorporado en el mapa de riesgos, el líder del proceso deberá reportarlo bajo el mismo procedimiento, realizar el análisis de causa raíz y evaluar, con acompañamiento de la segunda línea de defensa, su inclusión como nuevo riesgo en la matriz correspondiente.

Los colaboradores con rol y funciones de Planeación deben validar, consolidar y analizar los eventos de riesgos materializados reportados por los procesos o proyectos, y presentar en los casos requeridos, ante el Comité de Gestión y Desempeño aquellos que deban ser de su conocimiento y revisión. A través del Comité de Coordinación de Control Interno se realizará la verificación de la gestión realizada a los riesgos materializados.

12. MONITOREO

Primera línea de defensa

A través de autocontrol los funcionarios y contratistas de la primera línea de defensa realizan constante verificación de la gestión, los controles y planes de mitigación del riesgo. Se deberá realizar el reporte de seguimiento de manera cuatrimestral para riesgos para la integridad pública y semestral para riesgos de gestión, fiscales y de seguridad de la información.

Segunda línea de defensa

De acuerdo con la información reportada por la primera línea de defensa, Planeación analiza las situaciones asociadas a la gestión de riesgos en el marco de cambios, o necesidades de mejora que se deban gestionar en los riesgos de la entidad, informando a la primera línea sobre lo observado en los respectivos reportes.

Tercera línea de defensa

Este monitoreo lo gestiona el o la Profesional de Control Interno, quien realizará evaluación al cumplimiento de las acciones establecidas en los mapas de riesgos. De acuerdo con la programación del Plan anual de auditorías se analizará la efectividad de los controles asociados a los riesgos.

13. COMUNICACIÓN

Los profesionales de Planeación y Control Interno con el apoyo de Comunicaciones, coordinarán las acciones necesarias para promover la comunicación y divulgación de información orientada al fortalecimiento de la cultura de gestión integral del riesgo en la AND. Estas acciones se desarrollarán en concordancia con los objetivos estratégicos institucionales definidos en el Plan Estratégico Institucional, el Plan Estratégico de Comunicaciones y conforme a los lineamientos establecidos en la Política de Comunicación de la Entidad.

De igual forma, el proceso de Planeación coordinará la divulgación y publicación de los mapas de riesgos, considerando las necesidades de información de las partes interesadas y los canales institucionales definidos para tal fin, principalmente la Sede Electrónica y la Intranet.

Respecto a los riesgos de Seguridad de la Información, todas las novedades deberán ser comunicadas al Profesional de Seguridad de la Información y contar con la respectiva documentación de soporte, la cual podrá remitirse mediante correo electrónico u oficio. Asimismo, el o la Profesional de Seguridad de la Información deberá presentar dichas novedades ante el Comité Institucional de Gestión y Desempeño para su conocimiento, análisis y seguimiento.

Adicionalmente, la Agencia desarrollará al menos una (1) actividad anual de sensibilización y capacitación en gestión integral del riesgo dirigida a los colaboradores, liderada por el Profesional de Seguridad de la Información con el apoyo de Planeación, Control Interno y Comunicaciones, promoviendo el fortalecimiento de capacidades y la apropiación de la cultura de gestión del riesgo en todos los niveles de la organización, en armonía con el Plan Estratégico Institucional y la Política de Comunicación de la AND.

14. CUMPLIMIENTO

La presente Política se debe aplicar en todos los procesos y por todos los colaboradores de la Agencia.

15. VIGENCIA DE LA POLÍTICA

La política se revisará y actualizará, cuando se presenten cambios organizacionales, del entorno, operativos o normativos que afecten a la Entidad. Así mismo, se revisará cuando ocurran cambios de alcance que obliguen a su fortalecimiento, o de acuerdo

con los resultados de las actividades de seguimiento y control definidos. De igual manera, cuando sea necesario incluir las observaciones o recomendaciones presentadas por control interno en los informes de seguimientos, o los resultados de las evaluaciones llevadas a cabo por los organismos de control. En todo caso, se revisará como mínimo una (1) vez al año

CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	25/09/2018	Emisión del Documento
2	16/12/2019	Actualización del documento de acuerdo con el contexto de la Agencia.
3	11/10/2021	Actualización del objetivo, cambio del numeral de los etivos específicos, inclusión de definiciones, inclusión del nto 6 y 7, de acuerdo con la última versión de la Guía para administración del riesgo y el diseño de controles en idades públicas (versión 5). Función Pública, diciembre 20 y ajuste del numeral 9.
4	27/06/2024	Ajuste en redacción del objetivo y de los objetivos específicos; ampliación de definiciones (riesgo de seguridad digital y riesgo fiscal); referenciación de la Guía versión 6; eliminación de la referenciación de la Guía para la administración de riesgos de la AND; inclusión de misión, visión y objetivos estratégicos; ajuste de redacción sobre apetito y tolerancia; inclusión de estrategias para combatir el riesgo; inclusión del capítulo

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
		de roles y responsabilidades por línea de defensa; inclusión de roles para el oficial de seguridad de la información, subdirector jurídico y subdirector administrativo, en el marco de los requisitos FURAG; inclusión del capítulo de seguimiento y registro de riesgos materializados; inclusión del capítulo de monitoreo; ajuste de redacción del capítulo "Comunicación".
5	24/11/2025	Actualización del documento en los siguientes apartados: - Se incorpora la introducción del documento - Actualización de objetivos específicos - Actualización del alcance de la política - Referenciación de Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 7 - Se incorpora en el punto 8 la descriptiva de la gestión de riesgos - Gestión de Riesgos de Corrupción y LA/FT - Gestión de Riesgos Operacionales o de gestión - Gestión de Riesgos de Seguridad de la Información - Gestión de Riesgos Fiscales - Se adiciona la Revisoría Fiscal como parte de la tercera línea de defensa - Se incluye la declaratoria de la AND de cumplimiento
6	04/08/2026	Actualización integral de la política conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (DAFP, septiembre de 2025). Principales cambios: actualización del marco normativo y de referencia; ampliación de definiciones; sustitución del capítulo de riesgos de corrupción por los lineamientos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP; adopción del marco COSO-ERM y del modelo de madurez; redefinición de los niveles de apetito, tolerancia y capacidad diferenciados por tipología; incorporación de la tabla de criterios de probabilidad; incorporación de los criterios de identificación y descripción del riesgo, clasificación por factores, diseño y valoración de controles y cálculo del riesgo residual; incorporación de lineamientos de riesgos fiscales; incorporación de reglas de consolidación, actualización e

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
		inactivación de riesgos; incorporación de indicadores KRI y de control; armonización de las periodicidades de monitoreo y seguimiento; corrección de la numeración del capítulo 10; actualización de ISO/IEC 27001 a la versión 2022 y unificación de la denominación institucional.

Elaboró	Revisó	Aprobó
Andrés Mariño Ramírez Contratista - Gerente Anexo 01 Subdirección de Servicios Ciudadanos Digitales	Claudia P. Castaño S. Profesional de Planeación Tatiana Guerrero R. Profesional líder de comunicaciones Lady Gilari Torres Becerra Líder transversal – Subdirección de Servicios Ciudadanos Digitales Denis Fernando Montealegre Oficial de seguridad de la información	Maricela Torrenegra Directora (E) AND