Defensa

# GUÍA DE GESTIÓN INTEGRAL DE RIESGOS EN LA UNIDAD DE GESTIÓN GENERAL

## 2026

**VICEMINISTERIO PARA LA ESTRATEGIA Y PLANEACIÓN**

DIRECCIÓN DE PLANEACIÓN Y PRESUPUESTO

GRUPO DE GESTIÓN Y VALOR PÚBLICO

**Objetivo**: Establecer los lineamientos y criterios metodológicos para la gestión integral de riesgos que pertenecen a los sistemas de Gestión de la Unidad de Gestión General del Ministerio de Defensa Nacional, definiendo las etapas de identificación, análisis, valoración, monitoreo y tratamiento de los riesgos, con el fin de prevenir que su materialización afecte el cumplimiento de los objetivos institucionales.

**Alcance:** la presente guía es aplicable a todas las dependencias, procesos, sistemas de gestión, proyectos, programas y servidores públicos de la Unidad de Gestión General del Ministerio de Defensa Nacional, en todos los niveles jerárquicos y en las áreas misionales, estratégicas, transversales y de evaluación bajo el marco de gestión de riesgos.

| | |
|---|---|
| **Elaborado por:** | ***TE. Maira Gimena Botina Benavides*** |
| **Cargo:** | ***Asesora Grupo de Gestión y Valor Público*** |
| **Firma:** | ***Original debidamente firmado reposa en el archivo digital del Grupo de Gestión y Valor Público.*** |
| **Revisado por:** | **CT. Monica Soraya Castillo Gonzalez** |
| **Cargo:** | **Coordinadora Grupo de Gestión y Valor Público** |
| **Firma:** | ***Original debidamente firmado reposa en el archivo digital del Grupo de Gestión y Valor Público.*** |
| **Aprobado por:** | ***Gloria Stefany Cuesta Andrade*** |
| **Cargo:** | ***Directora de Planeación y Presupuesto*** |
| **Firma:** | ***Original debidamente firmado reposa en el archivo digital del Grupo de Gestión y Valor Público.*** |

**TABLA DE CONTENIDO**

## II. INTRODUCCIÓN

La gestión integral de riesgos es un componente esencial dentro del Sistema de Gestión y Desempeño Institucional (SGDI) y se desarrolla en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG) de la Unidad Gestión General del Ministerio de Defensa Nacional. Para garantizar la protección de los objetivos institucionales, se establecen una serie de lineamientos y criterios metodológicos enfocados en la administración efectiva de los riesgos que puedan afectar el desempeño de la entidad.

En este sentido la Unidad de Gestión General del Ministerio de Defensa Nacional (UGG) orienta su política de gestión del riesgo conforme a los lineamientos definidos en la Guía para la gestión integral del riesgo en entidades públicas, Versión 7, elaborada por el Departamento Administrativo de la Función Pública (DAFP). Esta guía, en adelante referida como la guía del DAFP, constituye el marco de referencia metodológico que la UGG adopta para diseñar, poner en marcha y fortalecer sus acciones en materia de gestión integral del riesgo.

La aplicación de la política de gestión del riesgo por parte de la UGG se desarrolla en armonía con los sistemas de gestión que la unidad ha implementado, así como con la normativa vigente aplicable. De esta forma, se asegura que la gestión del riesgo esté alineada con los estándares institucionales y legales, promoviendo así una administración coherente, eficiente y orientada al logro de los objetivos estratégicos definidos por la entidad.

En el ejercicio de la gestión institucional, es inevitable que surjan situaciones o eventos capaces de ocasionar desviaciones en el cumplimiento de los objetivos establecidos. Consciente de estos desafíos, la Unidad de Gestión General (UGG) desarrolla, a través de sus líneas de defensa, una serie de herramientas orientadas a reducir la probabilidad de ocurrencia o mitigar el impacto de la materialización de los riesgos. Para lograrlo, esta guía tiene como finalidad servir de instrumento de referencia y apoyo tanto para la Alta Dirección como para los servidores públicos y contratistas de la UGG, su objetivo es respaldar los esfuerzos orientados a robustecer las medidas preventivas y de control, fomentando una cultura institucional basada en el autocontrol, el respeto por la ética pública, la protección de los recursos asignados y la mejora continua del Sistema de Gestión y del Desempeño Institucional.

La Dirección de Planeación y Presupuesto, mediante el grupo de Gestión y Valor Público, proporciona a los líderes y responsables de los procesos la orientación, asesoría y acompañamiento metodológico necesarios para la aplicación eficaz de las herramientas de gestión del riesgo en todas sus etapas.

## III. MARCO NORMATIVO

| Nombre | Descripción |
|---|---|
| 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<br>Artículo 2. Objetivos del Sistema de Control Interno |
| Ley 610 de 2000 | Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías. |
| Ley 1474 de 2011 | Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. |
| Ley 1712 de 2014 | Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones |
| Ley 2195 de 2022 | Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones. |
| Decreto 1081 de 2015 | Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. |
| 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 1874 de 2021 | Por el cual se modifica la estructura del Ministerio de Defensa Nacional, se crean nuevas dependencias, funciones y se dictan otras disposiciones. |
| Decreto 1122 de 2024 | Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública. |
| Resolución 1621 de 2022 | Por el cual se adopta el Modelo Integrado de Planeación y Gestión y se integra el Modelo Estándar de Control Interno, se conforma el Comité de Gestión y Desempeño y el Subcomité de Coordinación del Sistema de Control Interno en la Unidad de Gestión General del Ministerio de Defensa Nacional y se derogan unas resoluciones. |
| Resolución 0545 de 2025 | Por el cual se modifica la resolución 2702 de 2023, se adopta el mapa de procesos de la Unidad de Gestión General del Ministerio de Defensa Nacional. |
| NTC-ISO 9001:2015 | Normas Técnica Colombiana, NTC ISO 9001-2015 |

| | |
|---|---|
| NTC – ISO 31000:2018 | Normas Técnica Colombiana, NTC ISO 31000:2018 |
| Guía para la gestión integral del riesgo en entidades públicas, Versión 7 | |
| Modelo Integrado de Planeación y Gestión V. 6.1 | |

## IV. GESTIÓN INTEGRAL DE RIESGOS EN LA UNIDAD DE GESTIÓN GENERAL

La Gestión Integral de Riesgos en la Unidad de Gestión General (UGG) del Ministerio de Defensa Nacional se articula de manera directa y transversal con el direccionamiento estratégico definido en el Plan Nacional de Desarrollo, la Política de Seguridad Defensa y Convivencia Ciudadana, el Plan Estratégico del Sector Defensa y Seguridad (PES) y el Plan Estratégico Institucional (PEI), asegurando coherencia entre la administración del riesgo, la planeación institucional y el logro de los objetivos estratégicos.

El Plan Estratégico del Sector Defensa y Seguridad constituye el marco de referencia sectorial para la materialización, seguimiento y monitoreo de la Política de Seguridad, Defensa y Convivencia Ciudadana, alineada con el Plan Nacional de Desarrollo "Colombia Potencia Mundial de la Vida". Este instrumento define las apuestas estratégicas del sector orientadas a la protección de la vida, la seguridad humana, la defensa del territorio, la protección del medio ambiente y el fortalecimiento de la Fuerza Pública. En este contexto, la gestión del riesgo permite identificar, evaluar y administrar los eventos que puedan afectar la ejecución de dichas estrategias, convirtiéndose en un habilitador de la efectividad de la política pública sectorial.

Por su parte, el Plan Estratégico Institucional, traduce los lineamientos sectoriales en acciones concretas a nivel de la UGG, definiendo objetivos, estrategias, indicadores y metas orientadas al cumplimiento de la misión institucional. Este plan está diseñado para dar cumplimiento al direccionamiento estratégico dispuesto por el Gobierno Nacional y se constituye en la hoja de ruta para orientar la gestión de la entidad. Así mismo, el PEI se encuentra estructurado bajo los mismos objetivos y ejes estratégicos de la política sectorial, garantizando la articulación con el nivel superior de planeación.

En este marco, la Guía de Gestión Integral de Riesgos establece los lineamientos metodológicos para identificar, analizar, valorar, tratar y monitorear los riesgos que puedan afectar el cumplimiento de dichos objetivos institucionales, asegurando su alineación con el Modelo Integrado de Planeación y Gestión (MIPG) y los sistemas de gestión implementados en la entidad. De esta manera, la gestión del riesgo no se concibe como un proceso aislado, sino como un componente estratégico que permea la planeación, la ejecución, el seguimiento y la evaluación institucional.

En síntesis, la gestión integral de riesgos en la UGG se encuentra estratégicamente alineada con la planeación sectorial e institucional, constituyéndose como un mecanismo fundamental para:

- Proteger el cumplimiento de los objetivos estratégicos institucionales.
- Fortalecer la toma de decisiones basada en información sobre riesgos.
- Garantizar la eficiencia, transparencia y generación de valor público.
- Asegurar la coherencia entre la planeación, la gestión y el control.

Esta articulación permite a la UGG consolidar un enfoque preventivo, proactivo y transversal de la gestión del riesgo, orientado a la mejora continua del desempeño institucional y al cumplimiento efectivo de las metas estratégicas del Sector Defensa.

*Figura 1. Alineación estratégica de la gestión integral de riesgos en la UGG*


*Fuente: Elaboración Grupo Gestión y Valor Público*

De acuerdo con las directrices establecidas por la Dirección Administrativa de Función Pública, el Ministerio de Defensa adopta los lineamientos metodológicos y los integra al Sistema de Gestión y Desempeño Institucional de la UGG.

Como se describe a continuación.

## 1. ALINEACIÓN ESTRATÉGICA DE LA GESTIÓN DEL RIESGO Y EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN MIPG.

El Modelo Integrado de Planeación y Gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, este modelo tiene como fin generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio. (Manual operativo MIPG, 2024, p. 9).

La Unidad de Gestión General del Ministerio de Defensa implementa el modelo de MIPG en sus 7 dimensiones y políticas que lo conforman, con el fin de generar resultados efectivos que atiendan los objetivos institucionales y resuelvan las necesidades y problemas de los Grupos de valor y ciudadanos, garantizando integridad, calidad en el servicio y eficiencia institucional.

En este contexto, la gestión de riesgos se configura como un componente esencial que articula todo el ciclo de planeación, gestión, seguimiento, evaluación y control. Esta alineación permite que la gestión de riesgos tenga impacto transversal en cada una de las dimensiones del MIPG, fortaleciendo la capacidad institucional para anticipar y mitigar posibles amenazas, así como para asegurar la continuidad y calidad en el cumplimiento de los objetivos estratégicos.

### DIMENSIÓN 1. TALENTO HUMANO

La dimensión de talento humano es el motor estratégico que atrae, desarrolla y potencia el capital humano para convertir las metas de la entidad en realidades sostenibles.

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| Gestión Estratégica del Talento Humano. | **Propósito de la Política:** Realizar seguimiento, análisis y evaluación sistemática de variables clave como el clima organizacional, el bienestar laboral, el desarrollo de competencias y el desempeño, con el fin de anticipar y mitigar riesgos institucionales, promoviendo entornos laborales saludables y soportar la toma de decisiones orientadas al logro de los objetivos de la entidad. |

| | |
|---|---|
| | **Marco de Riesgo:** Identificar, analizar y gestionar de manera preventiva los riesgos asociados al déficit o desalineación de competencias, la rotación y pérdida de talento, la desmotivación, el bajo desempeño y el desequilibrio en las cargas laborales, los cuales pueden afectar la continuidad operativa, la eficiencia institucional y el cumplimiento de los objetivos estratégicos, así como la calidad del servicio público prestado. |
| Integridad | **Propósito de la Política:** Promover, fortalecer y evaluar de manera sistemática el comportamiento ético, la transparencia y la confianza en la gestión institucional y con las partes interesadas que cada proceso identifica como grupos de valor e interés, con el fin de consolidar una cultura organizacional basada en la integridad, la responsabilidad y el servicio público.<br><br>**Marco de riesgo:** Identificar mecanismos preventivos y de control orientados a mitigar riesgos asociados a prácticas contrarias a la integridad, tales como conflictos de interés, fraude, corrupción y uso indebido de la información, así como aquellas conductas que puedan afectar la transparencia y la confianza institucional, promoviendo una cultura organizacional basada en valores, principios y conductas íntegras. |

## DIMENSIÓN 2. DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN

Desde el Direccionamiento estratégico se busca trazar la ruta institucional para transformar metas en resultados que generen valor público.

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| Planeación Institucional | **Propósito de la Política:** Medir, orientar y fortalecer la formulación, articulación, ejecución y seguimiento de los planes, programas y proyectos institucionales, garantizando coherencia entre la planeación estratégica, operativa y presupuestal.<br><br>**Marco de riesgo:** Identificar desarticulación entre planes, deficiencias en la formulación de objetivos e indicadores, cambios no gestionados y debilidades en el seguimiento. |
| Gestión Presupuestal y Eficiencia del Gasto Público | **Propósito de la Política:** Medir, fortalecer y optimizar la programación, ejecución, seguimiento y control de los recursos públicos, garantizando su uso eficiente, eficaz y transparente en cumplimiento de los objetivos institucionales. |

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| | **Marco de riesgo:** Identificar riesgos asociados a inadecuada programación presupuestal y ejecución ineficiente de recursos, retrasos en la contratación y reprocesos administrativos. |
| Compras y Contratación Pública | **Propósito de la Política:** Medir, fortalecer y optimizar la planeación, gestión y ejecución de los procesos contractuales, garantizando el cumplimiento del marco normativo, la transparencia, la eficiencia y la adecuada utilización de los recursos públicos.<br><br>**Marco de riesgo:** Identificar y mitigar riesgos asociados a fallas en la planeación contractual, incumplimientos normativos, selección inadecuada de contratistas y deficiencias en la supervisión. La administración del riesgo fortalece la transparencia, la legalidad y la efectividad de los procesos contractuales. |

## DIMENSIÓN 3. GESTIÓN CON VALORES PARA RESULTADOS

La gestión con valores busca ejecutar los planes institucionales con integridad, optimizando recursos para cumplirle al ciudadano.

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| Fortalecimiento Organizacional y Simplificación de Procesos | **Propósito de la Política:** Medir, fortalecer y optimizar de manera continua la estructura organizacional y los procesos institucionales, asegurando su alineación con la estrategia, el modelo de operación por procesos y las capacidades de la entidad, con el fin de incrementar la eficiencia, eficacia, coherencia y generación de valor público en la gestión de la entidad.<br><br>**Marco de riesgo:** Identificar, analizar y gestionar de forma preventiva los riesgos asociados a estructuras organizacionales desactualizadas o desalineadas con la estrategia institucional, la duplicidad o dispersión de funciones, desequilibrios en las cargas laborales, procesos no estandarizados, trámites innecesarios, reprocesos operativos y la resistencia al cambio organizacional, que puedan afectar la eficiencia institucional, la productividad, la calidad del servicio y el logro de resultados. |
| Servicio al Ciudadano | **Propósito de la Política:** Medir, fortalecer y mejorar la calidad, oportunidad, accesibilidad y efectividad de la atención brindada a la ciudadanía y a los grupos de valor e interés, garantizando un |

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| | relacionamiento cercano, incluyente y articulado, que contribuya a la satisfacción ciudadana, la confianza institucional y la generación de valor público.<br><br>**Marco de riesgo:** Identificar, analizar y gestionar de forma preventiva los riesgos asociados a deficiencias en los canales de atención dispuestos por la entidad; demoras o incumplimientos en la respuesta a solicitudes, PQRS y denuncias; atención inadecuada, inconsistente o no incluyente; debilidades en la articulación entre las áreas responsables del servicio; falencias en el seguimiento, evaluación y cierre oportuno de los compromisos adquiridos con la ciudadanía. |
| Participación Ciudadana en la Gestión Pública | **Propósito de la Política:** Vincular a la ciudadanía en todas las fases del ciclo de la gestión (diagnóstico, planeación, ejecución, seguimiento y evaluación). Garantizar que las decisiones públicas sean concertadas y transparentes, permitiendo que las personas influyan en la solución de sus problemas y ejerzan un control social efectivo sobre los recursos del Estado.<br><br>**Marco de riesgo:** Identificar y gestionar riesgos asociados a la limitada divulgación de los espacios y mecanismos de participación, uso de redes Sociales, baja representatividad de los grupos de valor e interés, deficiencias en la atención y respuesta a las solicitudes, peticiones, quejas, reclamos y sugerencias (PQRS), así como debilidades en el seguimiento a los compromisos adquiridos con la ciudadanía. |
| Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción | **Propósito de la Política:** Medir y fortalecer la publicidad, veracidad, oportunidad y accesibilidad de la información pública, así como prevenir prácticas contrarias a la legalidad y la ética administrativa.<br><br>**Marco de riesgo:** Identificar y gestionar riesgos asociados a la capacidad en la gestión institucional, la manipulación, alteración u ocultamiento de la información pública, el incumplimiento de los deberes de publicación y respuesta a solicitudes de información, la debilidad en los mecanismos de rendición de cuentas y la ineficacia de los canales de denuncia y control. |
| Gobierno Digital | **Propósito de la Política:** Promover el uso y aprovechamiento de las tecnologías de la información para transformar la relación del |

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| | Estado con el ciudadano, haciendo que los trámites sean ágiles y sencillos, y que la gestión pública sea más eficiente, transparente e innovadora para generar valor público<br><br>**Marco de riesgo:** Identificar riesgos asociados a fallas tecnológicas, ciberseguridad, disponibilidad de la información y bajo uso y adopción de herramientas digitales. |
| Seguridad Digital | **Propósito de la Política:** Proteger los activos de información y los sistemas tecnológicos de la entidad ante amenazas y riesgos cibernéticos, garantizando la confidencialidad, integridad y disponibilidad de la información y de los servicios digitales promoviendo un entorno digital confiable.<br><br>**Marco de riesgo:** Identificar y gestionar riesgos asociados a accesos no autorizados, divulgación, pérdida o manipulación indebida de información, ataques cibernéticos, indisponibilidad/interrupción de servicios y uso inadecuado de activos digitales, en articulación con los líderes de proceso y el SGSI |
| Defensa Jurídica | **Propósito de la Política:** Medir y fortalecer la prevención del daño antijurídico y la adecuada gestión de los procesos judiciales y administrativos, protegiendo los intereses del Estado.<br><br>**Marco de riesgo:** Identificar y gestionar riesgos asociados a la inadecuada gestión de procesos judiciales y administrativos, deficiencias en la defensa técnica, incumplimiento de términos procesales, debilidades en la articulación entre las áreas misionales y jurídicas, falta de análisis de precedentes y riesgos derivados de actos administrativos mal fundamentados. |
| Simplificación, Racionalización y Estandarización de trámites | **Propósito de la Política:** Esta política busca simplificar, estandarizar, eliminar y optimizar los procedimientos administrativos del Estado para reducir tiempos, costos y requisitos exigidos a los ciudadanos.<br><br>**Marco de riesgo:** Identificar puntos críticos en los trámites donde puedan presentarse riesgos de corrupción, sobornos o ineficiencias. |
| Mejora Normativa | **Propósito de la Política:** Fortalecer la generación de valor público mediante la formulación, revisión y actualización de normas de alta calidad regulatoria, claras, coherentes, eficaces y transparentes, |

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| | que respondan a las necesidades de la entidad y los grupos de interés, promuevan el bienestar social y el desarrollo económico sostenible, y contribuyan a la racionalización del acervo normativo.<br><br>**Marco de riesgo:** Gestionar de manera preventiva y sistemática los riesgos asociados al ciclo de producción normativa, incluyendo el riesgo de incumplimiento del marco legal y regulatorio, la emisión de normas ineficaces, incoherentes o desalineadas con los objetivos de política pública, la ausencia o deficiencia en análisis de impacto normativo, la falta de participación y consulta pública, y las debilidades en el seguimiento y evaluación normativa, que puedan derivar en sanciones legales, litigios, pérdida de legitimidad institucional, aumento de cargas administrativas innecesarias o afectaciones negativas al bienestar social y económico. |

## DIMENSIÓN 4. EVALUACIÓN DE RESULTADOS

Medir y analizar el desempeño institucional para aprender de los resultados y rendir cuentas con transparencia.

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| Seguimiento y Evaluación de la Gestión Institucional | **Propósito de la Política:** Medir, analizar y valorar el avance, los resultados y el impacto de la gestión institucional, a través de indicadores, metas y mecanismos de seguimiento que permitan apoyar la toma de decisiones, fortalecer la rendición de cuentas y promover la mejora continua.<br><br>**Marco de riesgo:** Identificar y gestionar riesgos asociados a la definición inadecuada de indicadores, ausencia de líneas base y metas claras, debilidades en las fuentes de información, retrasos en el reporte de resultados, inconsistencias en los datos y limitada articulación entre el seguimiento, la planeación institucional, el control interno y los planes de mejoramiento. |

## DIMENSIÓN 5. INFORMACIÓN Y COMUNICACIÓN

Garantizar el flujo efectivo de información de calidad para facilitar la gestión interna y fortalecer el diálogo con la ciudadanía.

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| Gestión Documental | **Propósito de la Política:** Garantizar que la información de la entidad sea íntegra, auténtica y esté organizada desde su creación hasta su disposición final. Su fin es facilitar la recuperación rápida de datos para la toma de decisiones, asegurar la preservación de la memoria institucional y garantizar el acceso ciudadano a la información pública de manera transparente y eficiente<br><br>**Marco de riesgo:** Identificar riesgos de pérdida, deterioro, desorganización y acceso no autorizado a la información, que afecte negativamente la integridad, disponibilidad y trazabilidad de los documentos institucionales. |
| Gestión de la Información Estadística | **Propósito de la Política:** Garantizar la producción, calidad, acceso, custodia y uso de datos confiables, relevantes y oportunos para la toma de decisiones basadas en evidencia, la planificación y la evaluación de políticas públicas<br><br>**Marco de riesgo:** identificar, valorar y mitigar riesgos de seguridad, privacidad e información estadística real y precisa (calidad de registros administrativos, cobertura, oportunidad). |

## DIMENSIÓN 6. GESTIÓN DEL CONOCIMIENTO Y LA INNOVACIÓN

Capturar, compartir y transformar el saber institucional en soluciones innovadoras que generen valor público.

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| Gestión del Conocimiento y la Innovación | **Propósito de la Política:** La Política de Gestión del Conocimiento y la Innovación del Ministerio de Defensa Nacional tiene como propósito medir, preservar y fortalecer la generación, apropiación, transferencia y uso del conocimiento institucional, con el fin de garantizar la continuidad operativa y promover la innovación en la gestión pública.<br><br>**Marco de riesgo:** Identificar riesgos asociados a la pérdida de conocimiento crítico, dependencia de la experiencia y conocimiento de personas clave, limitada o inexistente transferencia del conocimiento y baja innovación institucional. |

**DIMENSIÓN 7. CONTROL INTERNO**

Proveer seguridad razonable de que la gestión se alinea con la ley, las metas y la protección del patrimonio público.

| **Política MIPG** | **Alineación Estratégica con la gestión de riesgos** |
|---|---|
| Control Interno | **Propósito de la Política:** Garantizar que todas las actuaciones institucionales se ajusten a la ley, protejan los recursos públicos y aseguren el cumplimiento de las metas para generar confianza en la ciudadanía.<br><br>**Marco de riesgo:** Identificar y gestionar riesgos asociados a debilidades en el diseño, implementación y seguimiento de los controles internos, insuficiente segregación de funciones, falta de oportunidad en la identificación de riesgos emergentes, incumplimiento normativo y limitada efectividad de los planes de mejoramiento derivados de auditorías internas y externas. |

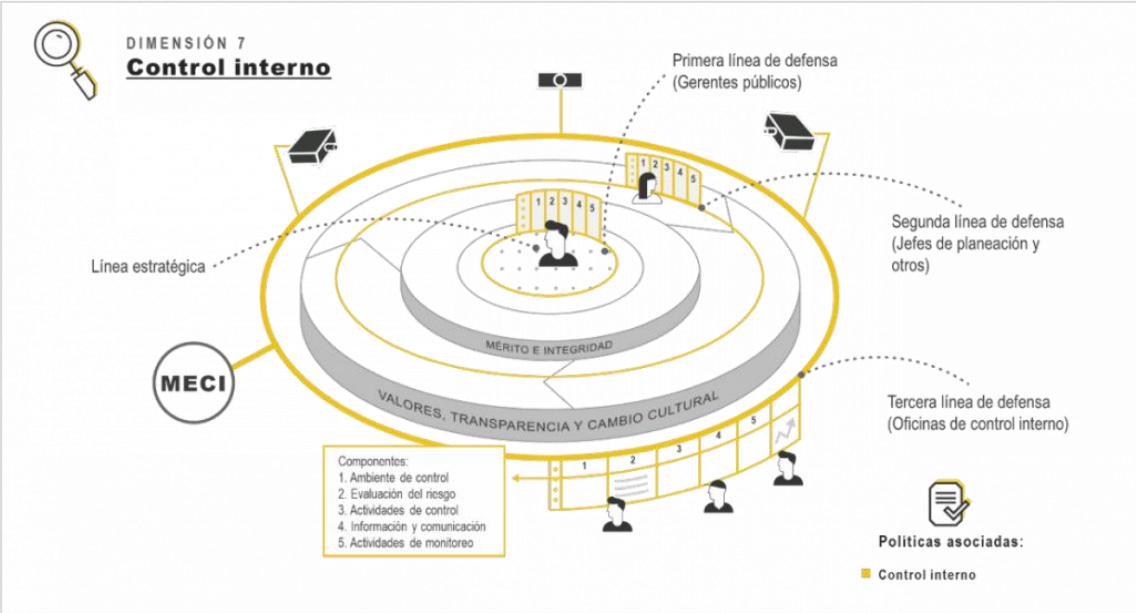
## 2. GOBERNANZA DE LA GESTIÓN DEL RIESGO (ESQUEMA DE LÍNEAS DE DEFENSA)

La Unidad de Gestión General adopta el esquema de Líneas de Defensa como mecanismo de gobernanza para la adecuada gestión, supervisión y evaluación de los riesgos institucionales, en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG) y la Dimensión de Control Interno. Este esquema permite delimitar responsabilidades, fortalecer el autocontrol y garantizar que la administración del riesgo se desarrolle de manera articulada, sistemática y efectiva en todos los niveles de la entidad.

La gobernanza del riesgo permite definir responsabilidades claras, fortalecer la toma de decisiones y asegurar que la administración del riesgo se desarrolle de manera estructurada, coherente y alineada con los objetivos institucionales.

El Modelo Integrado de Planeación y Gestión (MIPG) define para su operación articulada la creación en todas las entidades el Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Figura 2. Dimensión 7 - Líneas de Defensa




Fuente: DAFP

| **Línea estratégica – Nivel estratégico** |
|---|
| Está conformada por la Alta Dirección en el marco del Subcomité de Coordinación del Sistema de Control Interno. La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimiento a la gestión y auditoría interna para toda la entidad. |

| **Línea estratégica – Nivel estratégico** |
|---|
| El Comité Institucional de Gestión y Desempeño actúa como instancia estratégica de articulación entre la planeación institucional, el desempeño y la gestión integral del riesgo, en el marco del MIPG. |

**Tabla 1. Esquema líneas de defensa**

| **Primera línea de defensa – Nivel operacional** | **Segunda línea de defensa** | **Tercera línea de defensa** |
|---|---|---|
| Esta línea de defensa les corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad. Se debe precisar | Esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo, coordinador o asesor (Media o alta gerencia), quienes realizan labores de supervisión sobre | Esta línea de defensa está conformada por la Oficina de Control Interno, quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su |

| Primera línea de defensa – Nivel operacional | Segunda línea de defensa | Tercera línea de defensa |
|---|---|---|
| que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles de gerencia operativa, ya que son aplicados por líderes o responsables de proceso. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos. | temas transversales para la entidad y rinden cuentas ante la Alta Dirección. Aquí se incluyen a los jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros que se deberán definir acorde con complejidad y misionalidad de cada organización. Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección. | efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos o inadecuadamente cubiertos por la 2ª línea de defensa. |

*Nota: (...) actor puede hacer parte de varias líneas dependiendo del rol que asuma, ejemplo de ello es la Oficina Asesora de Planeación, que, por pertenecer al Comité Institucional de Coordinación de Control Interno, hace parte de la línea estratégica. Además, lidera el proceso de planeación, en tanto es primera línea de defensa, y también debe asesorar y cumplir labores de aseguramiento; razón por la cual, también es segunda línea de defensa.* De forma análoga se puede presentar este análisis para jefes o coordinadores de áreas como atención al usuario, TICs, contratación, financiera, así como otras que se identifiquen en este nivel, acorde con la complejidad y necesidades de cada entidad, Manual Operativo del MIPG V6.1 pág. 141 (2026).

***Fuente**. Elaboración propia basado en el Manual Operativo del MIPG V6 – Grupo de Gestión y Valor Público.*

## 2.1 LÍNEAS DE DEFENSA – UGG

Con el fin de asegurar que las responsabilidades y autoridades para la gestión del riesgo se asignan y comunican a los roles pertinentes, las siguientes responsabilidades de acuerdo con las líneas de defensa, así:

*Tabla 2. Funciones líneas de defensa UGG*

| LÍNEA DE DEFENSA | RESPONSABILIDADES |
|---|---|
| **Línea Estratégica / Nivel Estratégico** | • Definir la dirección estratégica y el marco de apetito y tolerancia al riesgo. |

| LÍNEA DE DEFENSA | RESPONSABILIDADES |
|---|---|
| • Despacho del Ministro de Defensa<br>• Despacho Viceministerios<br>• Secretarias (General y de Gabinete)<br>• Directores<br>• Jefes de oficina<br>• Dirección de Planeación y Presupuesto | • Asegurar la integración de la gestión del riesgo con planificación institucional y objetivos estratégicos.<br>• Revisar y analizar las propuestas presentadas por la Dirección de Planeación y Presupuesto, Grupo de Gestión y Valor Público relacionadas con la Política de Administración del Riesgo.<br>• Promover la administración de riesgos como un componente fundamental dentro de la operación de la UGG<br>• Realizar seguimiento periódico al cumplimiento de la Política de Administración de Riesgos definiendo acciones de mejora ante posibles desviaciones.<br>• Aprobar el marco de apetito de riesgo para la UGG y asegurar que sea coherente con los objetivos estratégicos establecidos.<br>• Supervisar el marco de apetito de riesgo con el objetivo de asegurar que se tomen las medidas adecuadas con respecto a niveles no aceptables.<br>• Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este.<br>• Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción correspondientes a los riesgos<br>• Supervisar el desempeño general de la gestión de riesgos e indicadores clave (KRI) y establecer acciones correctivas ante desviaciones. |
| **Primera línea de defensa / Nivel Operacional:**<br><br>• Líderes de proceso.<br>• Jefes de dependencia.<br>• Dirección de Planeación y Presupuesto | • Establecer y revisar el contexto institucional (interno y externo), así como definir las partes interesadas para su proceso.<br>• Asegurar que la construcción de los riesgos asociados al proceso se realice de forma participativa.<br>• Identificar, analizar, evaluar y valorar los riesgos de los procesos.<br>• Divulgar a todos los colaboradores a cargo el mapa de riesgos que contiene diferentes tipos correspondiente al proceso. |

| LÍNEA DE DEFENSA | RESPONSABILIDADES |
|---|---|
| | • Realizar monitoreo de los riesgos de acuerdo con lo establecido por el Grupo de Gestión y Valor Público.<br>• Asegurar la ejecución de los controles, su correcta documentación, aplicación, fortalecimiento e implementación de acciones de tratamiento sobre el riesgo.<br>• Realizar seguimiento periódico al comportamiento de los riesgos y en caso de su eventual materialización, realizar lo respectivo para declarar la materialización.<br>• Construir y actualizar el Mapa de Riesgos de proceso, integrando indicadores clave (KRI/KPI), cuando sea necesario.<br>• Comunicar alertas críticas cuando los indicadores clave KRI excedan umbrales aceptables.<br>• Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos según su tipología, |
| **Segunda línea de defensa**<br>• Comité Asesor de Contratación.<br>• Comité Paritario de Seguridad y Salud en el Trabajo (COPASST).<br>• Comité de Convivencia Laboral.<br>• Comités establecidos en la entidad para su correcto funcionamiento.<br>• Dirección de Planeación y Presupuesto.<br>• Directores<br>• Coordinadores<br>• Jefes de Oficina<br>• Gerentes de Proyectos | • Apoyar, orientar, supervisar y monitorear la gestión del riesgo realizada por la Primera Línea.<br>• Generar propuestas sobre la metodología y Políticas para la Administración del Riesgo de la Entidad y presentarlas para aprobación de la Alta Dirección.<br>• Coordinar, liderar, capacitar y asesorar a la primera línea de defensa en la aplicación de la metodología y políticas.<br>• Realizar un monitoreo independiente al cumplimiento de las etapas para la administración del riesgo.<br>• Consolidar el mapa de riesgos y socializarlo con las partes interesadas.<br>• Monitorear y consolidar los KRI definidos por la primera línea, analizando tendencias y criticidad.<br>• Proponer a la alta Dirección acciones para fortalecer y mejorar el resultado de Nivel de Madurez para la gestión del riesgo. |

| LÍNEA DE DEFENSA | RESPONSABILIDADES |
|---|---|
| **Tercera línea de defensa**<br>• Oficina de Control Interno. | • Apoyar en coordinación con la segunda línea de defensa la adecuada implementación de metodologías para la identificación y administración de los riesgos.<br>• Evaluar la efectividad y la aplicación de controles, así como también las actividades de monitoreo vinculadas a riesgos de la UGG.<br>• Verificar que los controles están diseñados e implementados de manera efectiva y operen de forma efectiva para mitigar los riesgos.<br>• Realizar seguimiento a las acciones establecidas en los planes de tratamiento en los procesos auditados.<br>• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.<br>• Realizar seguimiento a la administración de los riesgos consolidados en los Mapas de Riesgos en la entidad de conformidad con el Plan Anual de Auditoría y reportar los resultados al Subcomité de Coordinación de Control Interno de la UGG y al Comité de Coordinación del Sistema de Control Interno del Sector Defensa.<br>• Verificar que los indicadores (KRI) y controles sean pertinentes, suficientes y eficaces.<br>• Reportar hallazgos, brechas y recomendaciones a la Alta Dirección, y al Subcomité de Coordinación de Control Interno de la UGG y al Comité de Coordinación del Sistema de Control Interno del Sector Defensa.<br>• Hacer seguimiento al plan de acción derivado de auditorías y revisiones de riesgo. |

*Fuente. Elaboración propia – Grupo de Gestión y Valor Público.*

## 2.2 RESPONSABILIDADES EN LA ADMINISTRACIÓN DE LOS RIESGOS DE LA UGG.

- La Alta Dirección de la UGG, el Comité Institucional de Gestión y Desempeño y el Subcomité de Coordinación del Sistema de Control Interno[1] tienen la responsabilidad de:

  - Emitir, revisar y validar la política de gestión de riesgo y su cumplimiento, eficacia y mejora continua.
  - Orientar acciones para garantizar la gestión integral del riesgo de acuerdo con el resultado de nivel de madurez para la gestión de riesgos de la entidad.
  - Aprobar el apetito y la tolerancia al riesgo de la UGG, supervisar los indicadores clave de riesgo (KRI) y garantizar que la gestión de riesgos esté integrada con la planeación institucional y los objetivos estratégicos.
  - Someter a aprobación por parte del representante legal, la aprobación de la política de administración del riesgo y hacer seguimiento gestión integral de riesgos en el marco del literal g) del artículo 2.2.21.1.6 del Decreto 648 de 2017[2]

- Los líderes de Procesos y Equipos de Trabajo deben:

  - Administrar los riesgos a través de la ejecución de la metodología definida por el Grupo de Valor Público de la Dirección de Planeación y Presupuesto.
  - Diseña e implementa los controles, indicadores claves KRI/KPI, necesarios para disminuir la probabilidad de materialización de los riesgos.
  - Realizar el monitoreo de los riesgos junto con las evidencias de la ejecución sus respectivos controles.
  - Diseñar y ejecutar las actividades, las tareas y los planes de tratamiento y los planes de contingencia de acuerdo con lo establecido en los lineamientos.

- La Dirección de Planeación y Presupuesto, a través del Grupo de Gestión y Valor Público debe:

  - Emitir y estructurar la metodología para la gestión de los riesgos operativos y de corrupción de todos los procesos que hacen parte del Sistema de Gestión y Desempeño Institucional de la UGG.
  - Capacitar y acompañar a los procesos en la implementación de la metodología.
  - Consolidar el mapa de riesgos institucionales y de corrupción de la entidad
  - Realizar el informe cuatrimestral del monitoreo de los riesgos.

[1] Resolución 1621 de 2022 “Por el cual se adopta el Modelo Integrado de Planeación y Gestión y se integra el Modelo Estándar de Control Interno, se conforma el Comité de Gestión y Desempeño y el Subcomité de Coordinación del Sistema de Control Interno en la Unidad de Gestión General del Ministerio de Defensa Nacional y se derogan unas resoluciones”

[2] "^Artículo 2.2.21.1.6 Funciones del Comité Institucional de Coordinación de Control Interno. ''Son funciones del Comité Institucional de Coordinación de Control Interno: Son funciones del Comité Institucional de Coordinación de Control Interno: (...) g. Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta (...)."

- Asesora en la definición y actualización de los indicadores clave de riesgo (KRI) para todos los procesos de la entidad.
- Informar sobre los eventos y/o materialización de riesgos a las instancias correspondientes (Comité Institucional de Gestión y Desempeño y Subcomité de Coordinación del Sistema de Control Interno) para generar las acciones necesarias y evitar que se vuelva a materializar.
- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

- La Oficina de Control Interno Sectorial MDN debe:
  - Proporcionar información sobre la efectividad del Sistema de Control Interno a través de un enfoque basado en riesgos, incluida la gestión realizada por los diferentes responsables.
  - Evaluar la efectividad y la aplicación de controles en la gestión de los riesgos operativos y de corrupción.
  - Evaluar los planes de tratamiento, y planes de contingencia en caso de materialización.
  - Alertara a los miembros de la primera y segunda línea sobre la probabilidad de materialización de riesgos de gestión, fraude o corrupción en los procesos y/o dependencias auditadas.
  - Monitoreo del cumplimiento de los KRI como parte de su evaluación.

- Los Servidores públicos de la UGG y contratistas en general deben:
  - Ejecutar los controles y acciones definidas para la administración de los riesgos identificados.
  - Identificar y reportar los posibles riesgos que puedan afectar la gestión de los procesos de la UGG.
  - Participar activamente en el reporte cuatrimestral del monitoreo de los riesgos y cargue de las evidencias correspondientes a la ejecución de los controles y actividades adicionales de tratamiento.
  - Participar en la cultura de riesgo y sensibilización institucional.
  - Garantizar que sus reportes y evidencias sean oportunos y completos, para integrar al monitoreo de la segunda y tercera línea.

## 3. NIVELES DE MADUREZ PARA LA GESTIÓN DEL RIESGO

La gestión integral del riesgo, desde una perspectiva estratégica, comprende un conjunto de componentes interrelacionados que se consolidan progresivamente a partir de la cultura organizacional y se articulan con el direccionamiento estratégico, la planeación institucional y la toma de decisiones en todos los niveles de la entidad. En concordancia con lo anterior, resulta fundamental evaluar el nivel de madurez de la gestión del riesgo en la Unidad de

Gestión General como un elemento habilitador del desempeño institucional y del logro de los objetivos estratégicos.

Para tal fin, se adopta la herramienta de diagnóstico de madurez recomendada por el Departamento Administrativo de la Función Pública, basada en el marco COSO ERM 2017[3], el cual concibe la gestión del riesgo empresarial a partir de cinco componentes integrados y su relación directa con la misión, la visión y los valores institucionales. Esta herramienta permite valorar de manera estructurada el grado en que la gestión del riesgo se encuentra incorporada en la estrategia, los procesos, la cultura y los mecanismos de gobierno de la entidad.

El diagnóstico de madurez posibilita identificar el estado actual de la gestión integral del riesgo, determinando si esta se desarrolla de forma fragmentada o si, por el contrario, se encuentra efectivamente integrada en la planeación, la gestión y la evaluación institucional, así como en los procesos de toma de decisiones estratégicas. A partir de este análisis, se identifican brechas y temas a intervenir en una escala de severidad o prioridad para la atención al interior de la entidad.

Como resultado, el diagnóstico se constituye en un insumo clave para la formulación de un mapa de ruta orientado al fortalecimiento de la cultura de integridad, la transparencia, la ética pública, la gestión basada en información confiable y el mejoramiento continuo del desempeño institucional.

En la medida en que el diagnóstico de madurez trasciende su carácter evaluativo y se concibe como una herramienta de agilidad y aprendizaje organizacional, la entidad fortalece su capacidad de anticipación, respuesta y adaptación frente a los riesgos que pueden afectar el cumplimiento de su misión. Esta transformación se instrumenta técnica y operativamente mediante la ejecución de las siguientes dimensiones de análisis del diagnóstico (ANEXO 1. Herramienta Diagnóstico Modelo de Madurez UGG):

- ✓ **Gobierno y cultura:** La evaluación del nivel de madurez para la gestión del riesgo en este componente conceptualiza al gobierno en el marco de rendición de cuentas y la supervisión que la Alta Dirección ejerce sobre los riesgos. La cultura refleja las actitudes, percepciones y comportamientos compartidos por los funcionarios respecto al riesgo.

- ✓ **Estrategias y objetivos:** Este componente evalúa qué tan bien se integra la gestión de riesgos en la planificación de alto nivel de la entidad, a diferencia de la gestión operativa, el cual se enfoca en asegurar que los riesgos no se traten como una consideración aislada, sino un factor determinante en la toma de decisiones en la entidad.

[3] Guía para la gestión integral del riesgo en entidades públicas, versión 7-Función Pública – Agosto 2025- pág. 33

- ✓ **Desempeño**: Este componente se identifica como el motor operativo dentro del diagnóstico de madurez de riesgos. Su propósito es evaluar con qué eficacia la entidad identifica, analiza y responde a los riesgos en su día a día.

- ✓ **Análisis y monitorización:** Este componente del Modelo de Madurez actúa como el sistema de vigilancia de la entidad. Su objetivo es medir qué tan capaz es la entidad de detectar cambios en su entorno y evaluar si sus estrategias de mitigación están funcionando en tiempo real.

- ✓ **Información y comunicación**: Este componente busca garantizar que la información relevante sobre los riesgos fluya de manera oportuna, exacta y constante en todas las direcciones, a su vez evalúa si los datos utilizados para la gestión de riesgos son confiables y accesibles. En este nivel de madurez, se busca que la comunicación deje de ser un proceso administrativo para convertirse en un componente intrínseco que respalde la toma de decisiones informada.

*Figura No. 3. Componentes y principios evaluables modelo de madurez*

| Componente | Principios |
|---|---|
| Gobierno y Cultura | Supervisión de riesgos a través del consejo de administración. |
| | Establece estructuras operativas |
| | Define la cultura deseada |
| | Demuestra compromiso con valores clave |
| | Atrae, desarrolla y retiene a profesionales capacitados |
| Establecimiento de la estrategia y objetivos | Analiza el contexto (externo e interno) |
| | Define el apetito del riesgo |
| | Evalúa estrategias alternativas |
| | Formula objetivos estratégicos y operacionales |
| Desempeño | Identifica y describe el riesgo |
| | Evalúa el riesgo inherente |
| | Diseña controles efectivos |
| | Prioriza riesgos |
| | Desarrolla visión integral |
| Análisis y monitorización | Evalúa los cambios significativos |
| | Revisa el riesgo y el desempeño |
| | Persigue la mejora de la gestión del riesgo |
| Información, Comunicación y Reporte | Aprovecha la información y la tecnología |
| | Comunica información sobre riesgos |
| | Informa sobre el riesgo, la cultura y el desempeño |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7-DAFP*

Una vez realizada la evaluación integral de todos los componentes de análisis, los resultados obtenidos se integran en el mapa de calor, como se muestra en el ANEXO 1. Herramienta Diagnóstico Modelo de Madurez UGG (Mapa de calor). Este instrumento permite visualizar y categorizar los niveles de atención identificados según su criticidad:

máxima, alta, media y leve. El propósito principal de este ejercicio es transformar los hallazgos detectados en oportunidades de mejora para la entidad.

A partir de los resultados del mapa de calor, se procede a la formulación de un plan de intervención. Este plan está orientado a definir objetivos claros y acciones concretas que contribuyan a fortalecer, de manera progresiva y sostenible, el nivel de madurez institucional. Las acciones se diseñan considerando los diferentes niveles de atención, priorizando aquellas áreas que requieren intervención inmediata o significativa.

La Dirección de Planeación y Presupuesto, a través del Grupo de Gestión y Valor Público, liderará la implementación de la metodología descrita para la evaluación y actualización anual del nivel de madurez de riesgo institucional. Este proceso se desarrollará de manera articulada y participativa con las dependencias relacionadas, asegurando el compromiso y la colaboración de todas las áreas involucradas.

Adicionalmente, se presentará la propuesta de plan de intervención ante el Subcomité de Coordinación del Sistema de Control Interno, especialmente en aquellos componentes que, según el mapa de calor resultante de la evaluación, requieran atención máxima, alta y media. De esta forma, se garantiza una gestión dinámica y efectiva de los riesgos, promoviendo la mejora continua y el fortalecimiento institucional.

## 4. POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

### 4.1. Metodología de Construcción

La Unidad de Gestión General (UGG), en cumplimiento de los lineamientos establecidos en la Guía para la Gestión Integral de Riesgos, Versión 7, expedida por el Departamento Administrativo de la Función Pública, adopta y aplica la metodología allí definida, con el propósito de formular y establecer la Política Integral de Gestión del Riesgo de la entidad.

Para la estructuración y redacción de dicha política, la UGG se fundamenta en los siguientes componentes:

1. Compromiso y liderazgo de la Alta Dirección
2. Integralidad (Tipología de riesgos – Sistemas de gestión de la entidad)
3. Logro objetivos estratégicos
4. Objetivo de la política
5. Alcance de la política
6. Contexto interno y externo
7. Niveles de responsabilidad
8. Esquema metodológico

La Política Integral de Gestión del Riesgo de la UGG será única para la entidad y deberá ser acogida e implementada conforme a su alcance y objetivos institucionales. En cumplimiento de las funciones asignadas al Subcomité de Coordinación del Sistema de Control Interno de la Unidad de Gestión General del Ministerio de Defensa Nacional, dicha política deberá ser sometida a consideración y aprobación del Representante Legal de la entidad, cumpliendo este rol, el señor Ministro de Defensa Nacional.

## 4.2. Declaración de Política

*En el marco de lo estipulado en la Resolución No. 1621 de 2022, por la cual otorga funciones de aprobación al Subcomité de Coordinación del Sistema de Control Interno de la Unidad de Gestión General del Ministerio de Defensa Nacional – UGG se aprobó en abril del 2026 la declaración de la Alta Dirección y los propósitos institucionales frente a la Política para la Gestión Integral de Riesgos, como un componente estratégico, transversal y permanente de la gestión institucional.*

*La Unidad de Gestión General del Ministerio de Defensa Nacional – UGG se compromete a definir, implementar y mantener los lineamientos estratégicos y operativos que orienten la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos, en concordancia con lo establecido por el Departamento Administrativo de la Función Pública (DAFP), el Modelo Integrado de Planeación y Gestión – MIPG y las buenas prácticas internacionales de gestión de riesgos, en lo que resulte aplicable al contexto institucional.*

*La gestión integral de riesgos en la UGG comprende, entre otros, los riesgos estratégicos, operativos, fiscales, de integridad pública (Soborno, Fraude, Conflicto de Intereses, Corrupción, LA/FT/FP) de seguridad de la información y seguridad digital, ambientales, y de seguridad y salud en el trabajo, gestión de información estadística, así como aquellos riesgos emergentes derivados del contexto interno y externo. Estos riesgos serán gestionados mediante la definición e implementación de controles preventivos, detectivos y correctivos, así como planes y acciones de tratamiento orientados a la prevención, mitigación, administración y reducción del impacto de los riesgos, que puedan afectar el cumplimiento de los objetivos institucionales y la generación de valor público.*

*La presente política tiene como objetivo fortalecer la toma de decisiones informadas, promover el uso estratégico de la gestión del riesgo, asegurando la integridad, transparencia, eficiencia y uso adecuado de los recursos públicos. De igual manera, busca fomentar una cultura organizacional basada en la anticipación, la prevención y la gestión proactiva del riesgo, que apoye el cumplimiento de la misión institucional, la mejora continua del desempeño, asegurando la continuidad del servicio y/o la operación normal de la entidad en todos los escenarios de*

*materialización de riesgos y el fortalecimiento de la confianza ciudadana en la Unidad de Gestión General del Ministerio de Defensa Nacional.*

*Esta política tiene como alcance a todas las dependencias, procesos, proyectos, programas, sistemas de gestión y servidores públicos de la Unidad de Gestión General del Ministerio de Defensa Nacional, en todos los niveles jerárquicos y en las áreas misionales, estratégicas, transversales y de evaluación. La gestión integral de riesgos se incorpora de manera transversal en la planeación institucional, la ejecución presupuestal, la prestación de servicios, la adopción y uso de tecnologías, el fortalecimiento organizacional, así como en la formulación, ejecución y seguimiento de proyectos y programas institucionales. En este sentido la UGG tiene la obligación de mantener los documentos y registros de las contrapartes y sus operaciones por el término dispuesto en el artículo 12 de la Ley 2195 de 2022; y asignar los recursos técnicos, tecnológicos y de talento humano para poder llevar a cabo la gestión de los riesgos identificados.*

*La revisión de la presente política se realizará con una periodicidad anual en el marco de las sesiones del Subcomité de Coordinación del Sistema de Control Interno, o cuando se presenten actualizaciones sustanciales en la Guía para la Gestión Integral del Riesgo, en los objetivos institucionales o en el enunciado de la política. Para los ajustes derivados de la aplicación metodológica, actualización de herramientas o mejoras técnicas, se faculta a la Dirección de Planeación y Presupuesto, a través del Grupo de Gestión y Valor Público, en coordinación con el equipo de riesgos, para realizar las actualizaciones correspondientes, efectuar su liberación y garantizar su adecuada socialización al interior de la Entidad.*

## 5. APETITO DEL RIESGO

El apetito del riesgo representa el nivel de exposición al riesgo que la Unidad de Gestión General del Ministerio de Defensa Nacional está dispuesta a asumir en el desarrollo de sus funciones. Para determinar este parámetro fundamental, la entidad debe realizar una evaluación de aspectos clave, conforme a lo aprobado por la Alta Dirección en el marco del Subcomité de Coordinación del Sistema de Control Interno.

La identificación y análisis del apetito del riesgo deben estar alineados con la misión, visión, objetivos estratégicos y el mapa de operación por procesos de la entidad. Esta perspectiva integral permite comprender la naturaleza y el nivel de los riesgos a los que se enfrenta la organización, asegurando que la gestión se ajuste al contexto institucional y a las expectativas de sus grupos de interés.

### 5.1. Relación entre Riesgo y Desempeño

Resulta esencial entender cómo el riesgo impacta en el desempeño institucional. El monitoreo del desempeño actual posibilita identificar tendencias, relaciones y factores que inciden directamente en el perfil de riesgo de la entidad. Este análisis continuo permite anticipar posibles desviaciones y ajustar las estrategias de gestión para mantener el riesgo dentro de los límites definidos por la organización.

Gestión del Desempeño en el Contexto del Riesgo:

- Identificación de riesgos existentes y emergentes.
- Evaluación de la gravedad de cada riesgo identificado.
- Priorización de los riesgos en función de su impacto y probabilidad.
- Implementación de respuestas y controles para mitigar o administrar estos riesgos.
- Desarrollo de una visión integral a nivel de cartera, que facilite la toma de decisiones informadas y oriente la asignación eficiente de recursos.

Este enfoque estructurado fortalecerá la capacidad de la Unidad de Gestión General para anticiparse a los desafíos, responder de manera oportuna y asegurar el cumplimiento de sus objetivos institucionales a través de una gestión proactiva y responsable del riesgo.

A su vez la Guía para la gestión integral del riesgo en entidades públicas, versión 7- emitida por Función Pública, precisa en las definiciones que orientan la determinación del apetito del riesgo en las entidades públicas así:

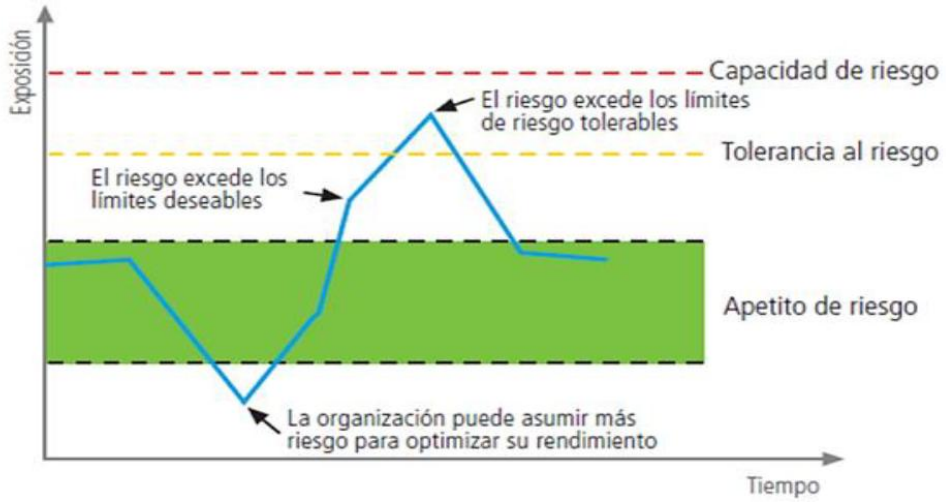
- **Apetito del Riesgo:** se refiere al nivel de riesgo que la entidad decide aceptar de manera consciente para lograr sus objetivos institucionales, teniendo en cuenta el marco legal, las directrices de la alta dirección y su misión. En otras palabras, es el punto de equilibrio que la entidad considera razonable entre arriesgarse y protegerse. Ejemplo: La Unidad de Gestión General decide que puede aceptar retrasos menores en algunos trámites administrativos (por ejemplo, hasta 5 días), si esto permite implementar mejoras en los procesos y optimizar recursos.

- **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. En otras palabras, la tolerancia al riesgo indica qué tanto puede desviarse la entidad del apetito de riesgo sin que la situación se considere inaceptable. Es decir, marca los márgenes permitidos alrededor del nivel de riesgo que se decidió asumir inicialmente Siguiendo el ejemplo anterior, si el apetito de riesgo es aceptar retrasos de hasta 5 días, la entidad podría definir que, de manera excepcional, tolera retrasos de hasta 7 días antes de activar alertas o acciones correctivas.

- **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. (relacionado con la solvencia y liquidez). En otras palabras, la capacidad de riesgo es el límite máximo que la entidad puede soportar antes de que el riesgo comprometa gravemente el cumplimiento de sus objetivos o

la estabilidad institucional. Superar este límite puede afectar la continuidad del servicio, la legalidad, la reputación o la sostenibilidad financiera de la entidad. Ejemplo. Si los retrasos en los trámites superan los 15 o 20 días y esto genera incumplimientos legales, sanciones o afecta la prestación del servicio a los ciudadanos, se estaría superando la capacidad de riesgo.

*Figura 4. Capacidad, límites y Tolerancia al Riesgo*




*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7-DAFP*

## 5.2. Metodología para definir el apetito del riesgo en la UGG:

La Unidad de Gestión General del Ministerio de Defensa define la metodología para establecer el apetito de riesgo de la entidad, con fundamento en declaraciones cualitativas, cuantitativas, y riesgos de tolerancia cero, en la medida en que este enfoque permite expresar de manera estructurada y coherente el nivel de riesgo que la entidad está dispuesta a asumir para el cumplimiento de su misión, objetivos estratégicos y responsabilidades institucionales, en armonía con su marco legal, su contexto operativo y los principios de la gestión pública.

Las declaraciones cualitativas posibilitan delimitar los tipos de riesgos aceptables y no aceptables, reflejando las expectativas de la Alta Dirección frente a aspectos estratégicos, reputacionales, éticos y de integridad pública. Por su parte, las declaraciones cuantitativas permiten establecer límites, umbrales e indicadores clave de riesgo que facilitan la medición, el seguimiento y el control de la exposición al riesgo, así como la evaluación de su impacto agregado sobre el desempeño institucional y la generación de valor público.

Asimismo, es importante considerar aquellos elementos del apetito de riesgo que no se pueden medir y que, por tanto, podrían ser más difíciles de gestionar, como los riesgos reputacionales. Todo ello se debe hacer de manera integral y equilibrada, de forma que las

medidas cuantitativas se combinen con las medidas cualitativas, como se ha definido en el Anexo 2.” Metodología para la definición del apetito del riesgo”.

El Anexo 2.” Metodología para la definición del apetito del riesgo”, define siete pasos que serán implementados por la UGG para definir el apetito de riesgo de la entidad, los cuales permiten que el apetito de riesgo adquiera la combinación de las declaraciones cualitativas con las cualitativas, se defina los riesgos de tolerancia cero y se alinee la gestión del desempeño con el contexto del riesgo, así:

1. **Alinear con objetivos institucionales:** Cuando un riesgo se encuentra directamente vinculado con la planeación institucional o compromete el cumplimiento de uno o varios objetivos estratégicos definidos en el Plan Estratégico Institucional, así como de los objetivos de proceso establecidos en el Modelo de Operación por Procesos de la entidad, dicho riesgo adquiere una connotación crítica para el logro de la misión institucional. En estos casos, la entidad establece una **aceptación nula del riesgo**, en la medida en que su materialización tendría un impacto extremo o catastrófico sobre el cumplimiento de los objetivos estratégicos y misionales.

2. **Categorizar los Tipos de Riesgo:** Se agrupan los riesgos para darles un tratamiento diferenciado, de acuerdo con su naturaleza y sistema de gestión vigente en la UGG, determinando su nivel de apetito bajo, moderado o de cero tolerancias según corresponda.

3. **Definir la Capacidad de Riesgo:** Es el límite máximo de pérdida o impacto que la Unidad de Gestión General del Ministerio de Defensa puede soportar antes de entrar en crisis técnica o financiera. Es el "techo" presupuestal o legal que no se puede sobrepasar en ninguna circunstancia.

4. **Determinar los Niveles de Apetito (Escalas):** Se establecen rangos cualitativos y cuantitativos: cero (No se acepta), Bajo (Se acepta con control estricto), Moderado (Se acepta bajo monitoreo) o extremo (Se asume para innovar o ganar eficiencia).

5. **Riesgos de tolerancia cero:** de acuerdo con el enfoque integral permite identificar aquellos riesgos frente a los cuales la entidad adopta una posición de tolerancia cero estos son: incumplimientos legales o regulatorios, seguridad de los servidores públicos, riesgos de fuerte impacto medio ambiental, y los de integridad pública.

6. **Establecer Tolerancias:** Los límites de tolerancia se definen como el margen permitido para que los procesos se desvíen del plan original sin afectar el objetivo general. Si este límite se sobrepasa, se activan los disparadores, los cuales funcionan como alertas de emergencia que obligan a intervenir de manera inmediata".

7. **Redactar la Declaración de Apetito:** Es el documento formal donde la Alta Dirección comunica cuánto riesgo está dispuesta a correr. Ej. La UGG tiene apetito nulo frente a

actos de corrupción, pero acepta riesgos moderados en la implementación de nuevas tecnologías administrativas".

8. **Monitoreo y Revisión Continua:** Dado que el entorno de seguridad y defensa cambia el apetito debe revisarse anualmente para asegurar que los niveles definidos sigan siendo realistas y seguros o cuando se presenten actualizaciones sustanciales en la Guía para la Gestión Integral del Riesgo, en los objetivos estratégicos institucionales de la entidad o en los objetivos de proceso, producto de actualizaciones o restructuraciones al interior de la UGG. Para los ajustes derivados de la aplicación metodológica, actualización de herramientas o mejoras técnicas, se faculta a la Dirección de Planeación y Presupuesto, a través del Grupo de Gestión y Valor Público, en coordinación con el equipo de riesgos, para realizar las actualizaciones correspondientes y efectuar su socialización al interior de la Entidad.

## *5.3. DECLARACIÓN APETITO DEL RIESGO EN LA UGG*

*En el marco de lo dispuesto en la Resolución No. 1621 de 2022, mediante la cual se asignan funciones de aprobación al Subcomité de Coordinación del Sistema de Control Interno de la Unidad de Gestión General del Ministerio de Defensa Nacional – UGG, en sesión realizada en abril de 2026 se aprobó la declaración de la Alta Dirección y los propósitos institucionales frente al apetito del riesgo, como un elemento estratégico que orienta la toma de decisiones y la gestión integral del riesgo en la entidad, sin perjuicio del cumplimiento de sus funciones institucionales, misionales y estratégicas.*

*La Unidad de Gestión General del Ministerio de Defensa Nacional – UGG establece una posición de tolerancia cero frente a aquellos riesgos cuya materialización tengan impacto extremo, que pueda afectar de manera directa el cumplimiento de la misión institucional y los objetivos estratégicos definidos en el Plan Estratégico Institucional, así como los objetivos derivados del Modelo de Operación por Procesos adoptado por la entidad. En este mismo sentido, la UGG declara tolerancia cero frente a:*

- *Riesgos de incumplimiento legal o regulatorio, que puedan generar sanciones, nulidades, pérdida de legitimidad institucional o responsabilidad disciplinaria, fiscal o penal.*
- *Riesgos que comprometan la seguridad y salud de los servidores públicos, poniendo en riesgo la vida, la integridad física o el bienestar laboral.*
- *Riesgos con impacto ambiental severo o irreversible, que afecten de manera significativa el entorno y generen pasivos ambientales para la entidad o el Estado.*
- *Riesgos de integridad pública, incluyendo actos de corrupción, soborno, fraude y conductas contrarias a la ética pública, incluyendo actos de corrupción, soborno, fraude, conflicto de intereses y cualquier conducta contraria a la ética pública y a los principios de transparencia.*
- *Riesgos que afecte la capacidad operativa de la Fuerza Pública o el presupuesto destinado a la defensa nacional.*

*Esta postura refleja el compromiso institucional con la legalidad, la integridad, la protección del recurso humano, la sostenibilidad ambiental y la generación de valor público.*

*Para los riesgos de gestión, riesgos fiscales, riesgos de seguridad de la información, Riesgos Ambientales de impacto controlable y riesgos asociados a la gestión de la información estadística, la UGG define un apetito de riesgo bajo a moderado, condicionado a que dichos riesgos no comprometan la continuidad de las operaciones críticas de la entidad. En particular, se consideran críticas aquellas operaciones relacionadas con:*

- *La ejecución y sostenibilidad financiera.*
- *El cumplimiento de los planes estratégicos y operativos.*
- *La adquisición oportuna de bienes y servicios esenciales.*
- *La disponibilidad, integridad y continuidad de los servicios de tecnologías de la información y las comunicaciones (TIC).*

*En estos casos, la aceptación del riesgo estará supeditada a la implementación de controles preventivos, detectivos y correctivos, así como a un monitoreo frecuente y sistemático, con tiempos de aplicación y responsables claramente definidos, de conformidad con la metodología establecida en la presente Guía.*

*En relación con la capacidad del riesgo, la UGG establece que aquellos riesgos que se ubiquen en zona de riesgo extremo, o cuya valoración cuantitativa represente un impacto igual o superior a 500 salarios mínimos mensuales legales vigentes – SMMLV, superan la capacidad de riesgo aceptable de la entidad. En consecuencia, estos riesgos deberán contar de manera obligatoria con planes de tratamiento formalmente definidos, y serán objeto de seguimiento y control reforzado por parte del Comité Institucional de Gestión y Desempeño y del Subcomité de Coordinación del Sistema de Control Interno de la UGG, hasta tanto se logre reducir su nivel de exposición a rangos aceptables.*

*Sin importar la valoración del riesgo, es decir: bajo, moderado, alto o extremo, el 100% de los riesgos identificados, deberán monitorear cuatrimestralmente sus controles de acuerdo con lo descrito en este documento, numeral 7. SEGUIMIENTO, MONITOREO Y REVISIÓN DE RIESGOS de la Presente Guía.*

## 6. GESTIÓN DEL RIESGO

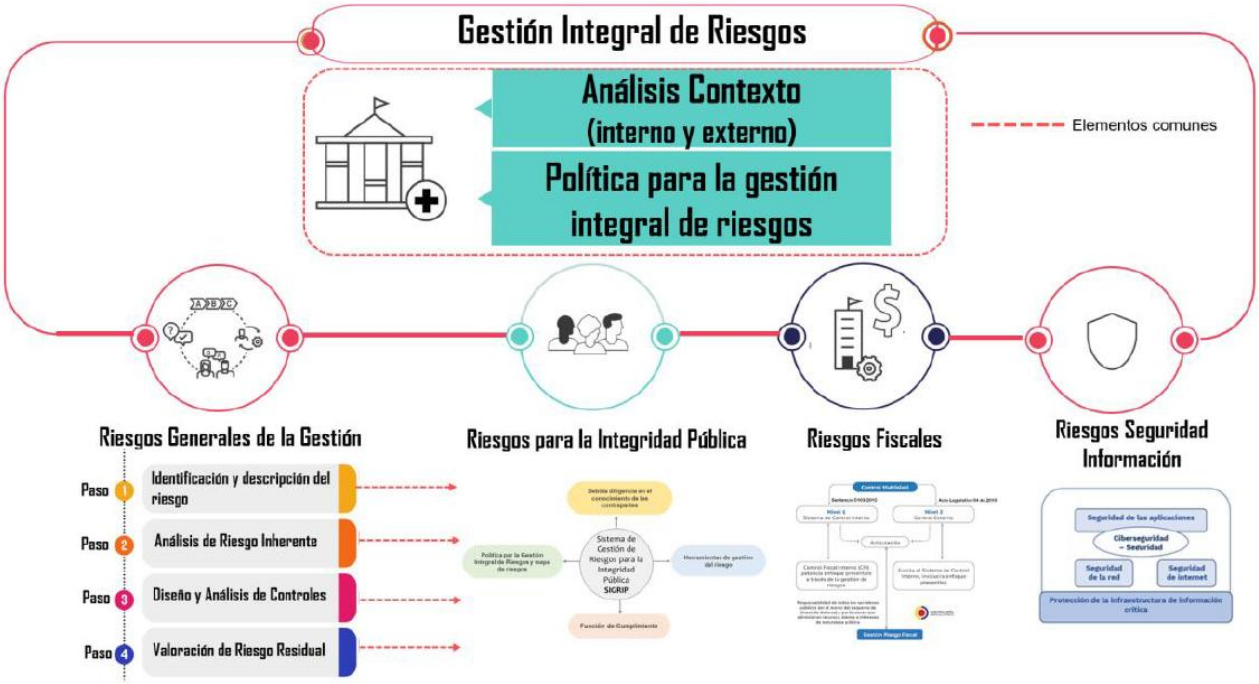
La Unidad de Gestión General del Ministerio de Defensa Nacional - UGG, en el marco del Modelo Integrado de Planeación y Gestión – MIPG y en cumplimiento de los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, desarrolla un análisis integral de los riesgos con el propósito de orientar acciones articuladas que contribuyan al cumplimiento de los objetivos estratégicos de la entidad.

Dicho análisis contempla la identificación, evaluación y tratamiento de los riesgos que puedan afectar el patrimonio público, comprometer la seguridad y confidencialidad de los activos de información, así como impactar negativamente la confianza, legitimidad

e imagen institucional, en especial aquellos asociados a conductas contrarias a los principios, valores y deberes del ejercicio del servicio público.

En concordancia con los lineamientos emitidos por el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, la Unidad de Gestión General adopta la siguiente articulación de ámbitos dentro del marco general para la gestión integral del riesgo, así:

*Figura 5. Articulación ámbitos gestión del Riesgo*




*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7-DAFP - Elaboración Dirección de Gestión y Desempeño Institucional. 2025*

Bajo estos ámbitos de articulación, la Unidad de Gestión General – UGG, en lo relacionado con el Marco de Riesgos, desarrollará e implementará una estructura metodológica única y estandarizada para toda la entidad, con el fin de garantizar un enfoque homogéneo, coherente e integral en la gestión del riesgo. Dicha estructura será de aplicación institucional, de conformidad con el alcance definido en la Declaración de la Política, establecida en el Numeral IV de la presente Guía.

Para su desarrollo, la metodología incorporará insumos y elementos comunes que aseguren una visión integral del riesgo, entre los cuales se destacan el análisis del contexto interno y externo, así como la articulación e integración de los sistemas de gestión implementados en la entidad. En este marco, la UGG adoptará de manera

transversal los pasos metodológicos establecidos para la gestión integral del riesgo, los cuales serán de aplicación general para todas las tipologías de riesgo desarrolladas en la presente Guía, a saber:

a. identificación y descripción del riesgo
b. análisis del riesgo inherente
c. diseño y análisis de controles
d. valoración del riesgo residual

La aplicación sistemática de esta metodología se encontrará descrita en el ***Anexo 3 "Metodología general para la gestión de riesgos"*** la cual permitirá fortalecer la toma de decisiones, facilitar la priorización de acciones y asegurar una gestión del riesgo consistente, orientada al logro de los objetivos estratégicos y al mejoramiento continuo del desempeño institucional.

### 6.1. TIPOLOGÍA DE RIESGOS CONSIDERADOS PARA LA GESTIÓN EN LA UNIDAD DE GESTIÓN GENERAL – UGG DEL MINISTERIO DE DEFENSA.

En atención al principio de integralidad de la gestión del riesgo, la Unidad de Gestión General (UGG) contempla la identificación y el tratamiento de once (11) tipos de riesgo, los cuales, de acuerdo con su naturaleza y características, pueden ser gestionados por los veinticuatro (24) procesos que conforman el Modelo de Operación por Procesos vigente en la entidad. No obstante, es importante precisar que la aplicabilidad de cada tipo de riesgo puede variar entre los procesos, en función del alcance y desarrollo de sus funciones, por lo que su incorporación en las matrices de riesgo se realiza de manera diferencial, sin que ello constituya una obligatoriedad para la adopción de la totalidad de los tipos de riesgo en todos los procesos.

1. **Riesgos Operativos y/o de Gestión:** refiere a la identificación y tratamiento de los riesgos asociados a la operación de la entidad, en otras palabras, corresponde a la posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos e impactan en toda la Entidad, comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la Entidad y de la articulación entre dependencias. (Metodología de identificación y tratamiento de acuerdo con Anexo 3)

2. **Riesgos Fiscales:** Son aquellos riesgos que puedan provocar daño patrimonial al estado de acuerdo con lo establecido en la "*Ley 610 de 2000, representado en el menoscabo, disminución, perjuicio, detrimento, perdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del estado".* (Metodología de identificación y tratamiento de acuerdo con Anexo 4)

3. **Riesgos de Seguridad de la Información:** Riesgos derivados de la posibilidad de pérdida, alteración, uso indebido, divulgación no autorizada o indisponibilidad de la información institucional, ya sea en formato físico o digital. Estos riesgos afectan la continuidad de los servicios y la confianza de los ciudadanos y grupos de valor. Se originan en vulnerabilidades tecnológicas, fallas en los controles de seguridad, errores humanos, amenazas internas o externas y deficiencias en la gestión de los activos de información. (Metodología de identificación y tratamiento de acuerdo con Anexo 5)

4. **Riesgos de Integridad Pública:** Corresponden a los riesgos asociados a conductas o situaciones que puedan afectar la probidad, transparencia, ética y legalidad en el ejercicio de la función pública, comprometiendo la confianza ciudadana, la legitimidad institucional y el cumplimiento de los fines del Estado. Se gestionan en el marco del Sistema de Gestión del Riesgo para la Integridad Pública (SIGRIP) y comprenden, entre otros, los siguientes: (Metodología de identificación y tratamiento de acuerdo con Anexo 6)

   a. **Riesgos de 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 actual. 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.*

   b. ***Riesgos de 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.*

   c. ***Riesgos de inadecuada gestión del conflicto de intereses:*** *surge cuando, 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*.[4]

   d. **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",

[4] Guía para la gestión integral del riesgo en entidades Públicas, Versión 7, Función Pública – Pag 116 -117

abuso del poder público para obtener beneficios privados, en contravención de los principios de legalidad, transparencia y moralidad administrativa, mediante prácticas como el soborno, la colusión, el tráfico de influencias, el peculado u otras conductas corruptas que afectan el interés general.

e. **Riesgos de LA/FT/FP - Lavado de activos (LA)/Financiación del Terrorismo (FT) / Financiación de la Proliferación de Armas de Destrucción Masiva (FP):** Corresponden a los riesgos derivados de la posibilidad de que la entidad sea utilizada, directa o indirectamente, como instrumento para ocultar, transformar, transferir o administrar recursos de origen ilícito, o para canalizar o destinar recursos a personas o grupos que puedan terminar atacando instituciones estatales, destinados a la financiación del terrorismo o de la proliferación de armas de destrucción masiva, afectando la legalidad, reputación y cumplimiento normativo institucional.

5. **Riesgos Ambientales:** Son aquellos riesgos asociados a la posibilidad de impactos negativos sobre el medio ambiente o el incumplimiento de obligaciones ambientales, derivados de las actividades, procesos, proyectos o decisiones de la entidad. Incluyen riesgos relacionados con el uso inadecuado de recursos naturales, la generación de impactos ambientales adversos, la gestión de residuos, el incumplimiento normativo ambiental y la exposición a riesgos derivados del cambio climático y otros factores del entorno. (Metodología de identificación y tratamiento de acuerdo con Anexo 3)

6. **Riesgos de Salud y Seguridad en el Trabajo:** Corresponden a los riesgos relacionados con la posibilidad de ocurrencia de accidentes de trabajo, enfermedades laborales o afectaciones a la salud física y mental de los servidores públicos, contratistas y demás partes interesadas, como consecuencia de condiciones inseguras, actos inseguros o deficiencias en la gestión del Sistema de Seguridad y Salud en el Trabajo. Su materialización puede afectar el bienestar del talento humano, la continuidad operativa y el desempeño institucional. (Metodología de identificación y tratamiento de acuerdo con Anexo 7)

7. **Riesgos de Gestión Estadística:** Son aquellos riesgos asociados a la posibilidad de que la información estadística producida, administrada o utilizada por la entidad sea inexacta, incompleta, inconsistente, inoportuna o no confiable, afectando la toma de decisiones, la formulación de políticas públicas, la planeación institucional y la rendición de cuentas. Se originan en debilidades en los procesos de recolección, procesamiento, análisis, difusión y uso de la información estadística. (Metodología de identificación y tratamiento de acuerdo con Anexo 3)

# 7. SEGUIMIENTO, MONITOREO Y REVISIÓN DE RIESGOS

## 7.1. INDICADORES CLAVE DE RIESGO (KRI)

En este literal se tienen en cuenta las bases conceptuales para el diseño y seguimiento a los Indicadores Clave de Riesgo (Key Risk Indicators – KRI por sus siglas en inglés), los cuales surgen como una herramienta fundamental para la toma de decisiones informadas, al suministrar información sobre riesgos emergentes y potenciales, así como eventos o puntos desencadenantes por situaciones externas que pueden tener impacto sobre el logro de los objetivos de la entidad. (DAFP 2025)

**Tipologías de Indicadores para el seguimiento**

Para definir los indicadores clave de riesgo, es necesario partir desde el despliegue de la plataforma estratégica de la entidad (Misión, visión y valores fundamentales), esta es la base para la formulación de objetivos estratégicos que orientan la planeación y permiten un despliegue hacia los objetivos de los procesos (Desde lo más estratégico a lo más operativo).

Es importante en este punto aclarar que la Guía para la Construcción de Indicadores V4 de la Función Pública, establece una tipología de indicadores orientada a medir el desempeño institucional, teniendo en cuenta que clasifica los indicadores en: eficiencia, eficacia, efectividad, economía y calidad, además, esta guía define los tipos de evaluación y cómo los indicadores se aplican desde el nivel estratégico hasta los procesos, programas y proyectos, permitiendo hacer seguimiento al cumplimiento de los objetivos de la entidad. Por su parte, la Guía para la Gestión Integral del Riesgo V7, plantea **las tipologías de indicadores para el seguimiento**, enfocándose más en cómo estos indicadores se utilizan dentro de la gestión del riesgo, articulando los indicadores de desempeño (KPI) con los indicadores clave de riesgo (KRI) para apoyar el monitoreo y control.

En este sentido, para la definición de los indicadores clave de riesgo (KRI) en la UGG, se tendrán en cuenta los tipos de indicadores definidos tanto en la Guía de Indicadores V4 de Función Pública, como en la Guía Indicadores de Gestión de la UGG DP-G-004, con el fin de mantener coherencia en la formulación y medición de los indicadores KRI.

La figura 6 representa la forma como se vinculan los indicadores clave de riesgo con los indicadores clave de proceso.

*Figura 6. Articulación indicadores clave de riesgo y los indicadores clave de proceso*


*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7-DAFP – Adaptado por la Dirección de Gestión y Desempeño Institucional. 2025*

**Qué es un indicador Clave de Riesgo (KRI):** Métricas utilizadas por la entidad para proporcionar una señal temprana de exposiciones al riesgo, cada vez mayores en diversas áreas de la organización (COSO). 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. Son una herramienta potencial para el seguimiento y monitoreo de los riesgos, ya que pueden entregar de forma cualitativa o cuantitativa señales de alerta temprana, así como detectar tendencias o cambios en los niveles del riesgo, lo que facilita que se incorporen acciones correctivas y preventivas para minimizar sus impactos frente a posibles materializaciones.

**Que es un indicador clave de proceso (KPI)** Son métricas que permiten medir de manera periódica el desempeño de los procesos de una entidad, en relación con el cumplimiento de

sus objetivos y metas establecidas. Se utilizan para evaluar la eficacia, eficiencia y efectividad de los procesos, facilitando el seguimiento a los resultados y la toma de decisiones.

**Alcance de los indicadores clave de proceso (KPI) y los indicadores clave de riesgo (KRI)**

Cada uno de estos indicadores presentan unas diferencias, pero resultan complementarios en el **análisis**, la guía de la Función Pública sugiere que los indicadores KRI deben comunicarse junto con los indicadores KPI lo que presenta una relación entre el riesgo y el desempeño.

Respecto de los indicadores KPI son los que actualmente están definidos en cada uno de los 24 procesos que hacen parte del modelo de operación por procesos de la entidad y que son monitoreados en la plataforma Suite Visión Empresarial-SVE, por ejemplo, porcentaje de productos del proceso de defensa y seguridad realizados, oportunidad, de respuesta de trámites de reconocimientos prestacionales y/o pensionales, nivel de satisfacción de los usuarios de la oferta de bienestar.

Para los indicadores KRI, se tendrá en cuenta la metodología de formulación y medición definida para la entidad, asegurando que estén alineados con la gestión de los riesgos y así evaluar la efectividad de los controles.

*Tabla 3. Alcance aplicación KPI y KRI*

| 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 requieren mayores recursos y atención. | Ayudan a identificar y anticipar problemas que se pueden presentar 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 | Facilitan el proceso de generación de informes y el escalamiento de los riesgos. |

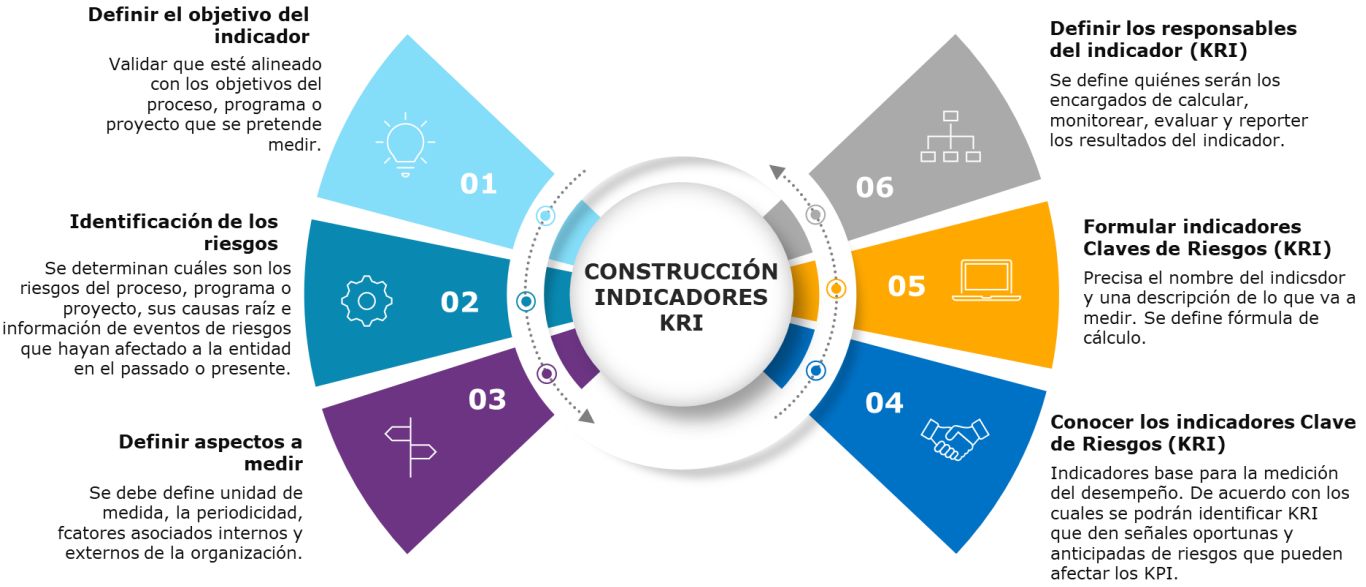
| | |
|---|---|
| de las acciones, logrando tomar decisiones con mayor certeza y confiabilidad | |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7-DAFP – Adaptado por la Dirección de Gestión y Desempeño Institucional. 2025*

## Pasos para la definición y construcción de indicadores KRI

La guía de la función pública propone 6 pasos para la construcción de los indicadores, aun así, se debe tener en cuenta que esta metodología para la formulación de indicadores no puede ser ajena a la metodología que tiene la entidad a través del documento DP-G-004 Guía de indicadores de la UGG.

Figura 7. Pasos para la construcción de KRI




*Fuente: Elaboración con base en la figura 31 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025)*

Para la construcción de los indicadores KRI, como se mencionó anteriormente, es indispensable tener en cuenta la metodología de indicadores definida en la entidad, y por lo menos debe contemplarse:

1. Objetivo del indicador que debe estar alineado a lo que se quiere medir; 2. Identificar el riesgo que haya afectado a la entidad en el pasado o presente; 3. Aspectos a medir en donde se establece unidad de medida, periodicidad, los factores internos o externos de la entidad y especialmente, que se pretende medir; 4. Conocer los indicadores KPI; 5, Formular el indicador KRI en donde se precisa como mínimo lo siguiente (i. El nombre del indicador, ii. una descripción de lo que se va a medir, iii. la fórmula de cálculo, iv. 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, v. frecuencia de medición y seguimiento y; vi. umbrales de alerta),

*Tabla 4. Ejemplo Indicadores Clave de 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 |
| TALENTO HUMANO | Rotación de personal | % de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses |

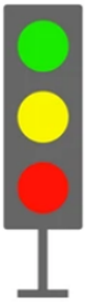
*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7-DAFP – Adaptado por la Dirección de Gestión y Desempeño Institucional. 2025*

**Umbrales de alerta**

Es necesario definir los umbrales de alerta ya que no todos los cambios en los KRI requieren acción inmediata, para ello en primera instancia el líder del proceso, plan, programa o proyecto define estos umbrales para priorizar las áreas de la entidad que requieren intervención inmediata y distinguirlas de aquellas situaciones donde los riesgos están bajo control.

Aunque la guía para la gestión integral del riesgo V7, plantea una semaforización que permite distinguir entre valores aceptables, riesgosos o críticos, así:

*Figura 6. Semaforización para distinguir los valores*



**Valor Bajo (Verde):** Valor mínimo deseado.

**Valor Moderado (Amarillo):** Valor que indica riesgo potencial.

**Valor Alto (Rojo)**: Valor crítico o inaceptable.

*Fuente: Elaboración con base en la Guía para la gestión integral del riesgo en entidades públicas, versión 7-DAFP*

En la UGG se adapta la escala de evaluación definida en la guía de indicadores de la entidad y que se encuentra parametrizada en la SVE.

*Figura 7. Escala de evaluación UGG*


*Fuente: Guía de Indicadores de Gestión de la UGG - DP-G-004.V2*

**Indicadores KRI y la relación con el apetito del riesgo**

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:**

| Apetito del riesgo | KRI | KRI |
|---|---|---|
| Hasta 10 quejas de usuarios al mes | 8 quejas (Cerca del umbral) | 12 quejas (Excedió el apetito) - Implementación de medidas correctivas. |

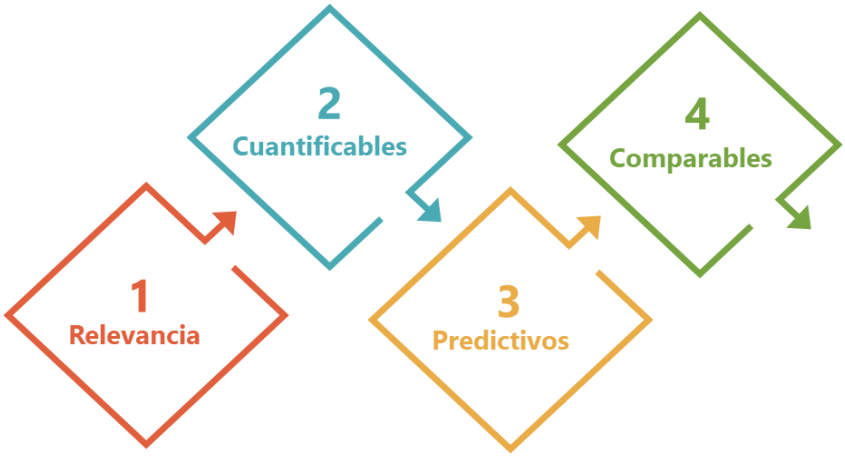
**Recomendaciones en la formulación de los indicadores KRI**

- Definir quiénes serán los encargados de calcular, monitorear, evaluar y reportar los resultados del indicador.

- Para una mayor efectividad a la hora de identificar y formular los indicadores KRI, se deben tener en cuenta las siguientes recomendaciones:

    - Relevancia: Deben estar alineados con los riesgos críticos para la entidad. (Estos serán los que se hayan determinado en el paso 1 de identificación y descripción del riesgo).
    - 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.

*Figura 8. Recomendaciones para una mayor efectividad*




*Fuente: Elaboración con base en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025)*

- 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.

**Comunicación y reporte de indicadores KRI**

Teniendo en cuenta el esquema de líneas de defensa de la UGG, se requiere que cada rol identificado contribuya a la generación de alertas tempranas para fortalecer la gestión del riesgo y evitar la materialización.

| Líneas de Aseguramiento | Responsable | Responsabilidad Frente a los Indicadores KRI |
|---|---|---|
| Línea Estratégica | Subcomité de Coordinación del Sistema de Control Interno<br><br>Alta dirección:<br>Despacho del ministro de Defensa<br>Despacho Viceministerios<br>Secretarias (General y de Gabinete)<br>Directores<br>Jefes de oficina<br>Oficina de control Interno Sectorial<br>Dirección de Planeación y Presupuesto<br><br>Comité de Gestión y Desempeño Institucional | Incorporar en la política para la gestión integral de riesgos lineamientos sobre los Indicadores Clave de Riesgo (KRI).<br><br>Realizar seguimiento y análisis periódico a los indicadores claves de riesgos institucionales y proponer mejoras a su estructura.<br><br>Analizar los umbrales definidos para los Indicadores Clave de Riesgo (KRI) y sugerir ajustes de ser necesario, de tal forma que estos se alineen con los niveles aceptables para la entidad.<br><br>Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a los indicadores claves de riesgo, así como a los indicadores clave de proceso asociados.<br><br>Realizar seguimiento y análisis periódico a los indicadores claves de desempeño de manera articulada con los indicadores clave de riesgo.<br>Generar las alertas que correspondan, de acuerdo con los umbrales definidos para los Indicadores Clave de Riesgo (KRI). |
| 1ª Línea de Aseguramiento | Líderes de proceso.<br>Jefes de dependencia.<br>Dirección de Planeación y Presupuesto | Identificar y formular los indicadores clave de riesgos que pueden alertar sobre la exposición al riesgo para los procesos, programas o proyectos bajo su responsabilidad.<br><br>Aplicar, medir y hacer seguimiento a los indicadores clave de riesgos, alineados con los indicadores clave de proceso.<br><br>Reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos de acuerdo con los indicadores claves de riesgo dentro de los plazos establecidos.<br><br>Informar a la Oficina Asesora de Planeación o quien haga sus veces (como 2ª línea de defensa) sobre las alertas críticas resultado de la medición de los indicadores claves de riesgo bajo su responsabilidad. |

| Líneas de Aseguramiento | Responsable | Responsabilidad Frente a los Indicadores KRI |
|---|---|---|
| | | Si se identifica que un indicador claves de riesgo está fuera del umbral esperado, la primera línea de defensa debe actuar para corregir las desviaciones identificadas.<br><br>Establecer y aplicar las acciones de mejora requeridas para optimizar la operación de los procesos, planes, programas o proyectos de acuerdo con los resultados de las métricas aplicadas. |
| 2ª Línea de Aseguramiento | Comité Asesor de Contratación.<br>Comité Paritario de Seguridad y Salud en el Trabajo (COPASST).<br>Comité de Convivencia Laboral.<br>Comités establecidos en la entidad para su correcto funcionamiento.<br>Dirección de Planeación y Presupuesto.<br>Directores<br>Coordinadores<br>Jefes de Oficina<br>Gerentes de Proyectos | Asegurar que los indicadores claves de riesgo estén alineados con los objetivos estratégicos y operativos de la entidad.<br><br>Proponer la inclusión de los lineamientos en materia de indicadores claves de riesgo en la estructura de la política para la gestión integral de riesgos, para aprobación por parte de la Alta Dirección.<br><br>Establecer las metodologías que guíen la medición, seguimiento y monitoreo de los indicadores claves de riesgo, asegurando que se utilicen las mejores prácticas y se implementen de manera efectiva.<br><br>Consolidar los indicadores claves de riesgo con mayor criticidad frente al logro de los objetivos y presentarlos periódicamente (establecer una periodicidad concreta) ante la Línea Estratégica para su análisis y toma de decisiones.<br><br>Asesorar y supervisar a la 1ª línea para la correcta identificación, formulación e implementación de los indicadores claves de riesgo. |
| 3ª Línea de Aseguramiento | Jefe Oficina Asesora de Control Interno | Verificar si los indicadores claves de riesgo están definidos y se aplican por parte de los responsables.<br><br>Evaluar si los indicadores claves de riesgo son pertinentes y eficaces para la oportuna generación de alertas y/o implementación de correctivos.<br><br>Informar a la Alta Dirección en coordinación con la 2ª línea, cuando se detecten deficiencias o brechas en los indicadores claves de riesgo |

| Líneas de Aseguramiento | Responsable | Responsabilidad Frente a los Indicadores KRI |
|---|---|---|
| | | para que tomen decisiones sobre las medidas preventivas y correctivas que deben implementarse.<br><br>Asesorar y acompañar a la Alta Dirección en el análisis de los resultados de los indicadores claves de riesgo, así como en la incorporación de estrategias para la identificación y monitoreo estratégico de los indicadores claves de riesgo. |

*Fuente: Adaptado con base en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025)*

## 7.2. MONITOREO DE RIESGOS

El monitoreo o seguimiento a la administración de riesgos se realiza en primera instancia por el responsable del proceso y en instancias posteriores por las auditorías internas de calidad o de gestión programadas por la Oficina de Control Interno. La finalidad principal de éstas es verificar las disposiciones de monitoreo y sugerir los correctivos u oportunidades de mejora para los ajustes necesarios a los riesgos identificados.

El monitoreo es un ejercicio que pretende una revisión a toda la gestión de los riesgos, lo que significa un recorrido desde la identificación, análisis de riesgo inherente, controles, evaluación de controles, calificación de los riesgos después de aplicación de controles (riesgo residual); el objetivo consiste en realizar los ajustes y correcciones necesarios en el caso que se requiera. En el caso que exista un cambio de denominación e identificación del riesgo será necesario explicar el porqué de este cambio

En el monitoreo del riesgo debe responder a las siguientes preguntas:

| N° | Pregunta | Respuesta |
|---|---|---|
| 1 | ¿El proceso se ha desarrollado sin cambios significativos durante los últimos 4 meses? | SI/No explique su respuesta |
| 2 | ¿El riesgo sigue siendo vigente de acuerdo con el alcance del proceso? | SI/No explique su respuesta |
| 3 | ¿la institución ha sufrido algún cambio significativo que afecte la identificación del Riesgo? | SI/No/N. A |
| | ¿El proceso ha sido auditado durante el último trimestre, y ha recibido alguna recomendación especifica? | SI/No explique su respuesta |
| 4 | ¿La aplicación de los controles ha resultado ser efectiva, es decir, el riesgo no se ha materializado? | SI/No |
| 5 | ¿El proceso cuenta con los soportes de la aplicación de los controles? | SI/No |

| N° | Pregunta | Respuesta |
|---|---|---|
| 6 | ¿Las acciones de tratamiento se han desarrollado oportunamente? | SI/No/N. A |

El responsable del monitoreo debe responder dichas preguntas a través de un párrafo o comentario y adjuntar los soportes necesarios

De igual manera en respuesta a la dimensión 7 del MIPG, Control Interno, esta etapa de la gestión del riesgo se desarrolla de la siguiente manera:

A) Líderes de proceso y sus equipos de trabajo: Efectuar el monitoreo de los riesgos y su respectivo reporte con una periodicidad cuatrimestral de acuerdo con las siguientes fechas de corte:

- Primer monitoreo: reporte de monitoreo con corte a 30 de abril de cada año
- Segundo Monitoreo: corte a 31 de agosto
- Tercer monitoreo: corte a 31 de diciembre

El reporte de monitoreo se debe hacer a más tardar 10 días calendario después de cada fecha de corte y se realiza en la SVE como parte final de todas las etapas de la administración del riesgo. El proceso que incumpla los tiempos de monitoreo deberá aperturar obligatoriamente una oportunidad de mejora- OM en el SGDI – SVE. (Revisión y eficacia por parte del Grupo GVP)

Se deben cargar los soportes que permitan evidenciar la revisión a toda la gestión de los riesgos, lo que significa un recorrido desde la identificación, análisis de riesgo inherente, controles, evaluación de controles, calificación de los riesgos después de aplicación de controles (riesgo residual)

B) Dirección de Planeación y Presupuesto, Grupo de Gestión y Valor Público y coordinadores de los Sistemas de Gestión: realiza un seguimiento cuatrimestral y presenta un informe que resume los resultados del monitoreo realizado por la primera línea de defensa, dirigido a la Alta Dirección y a los líderes de proceso y directores.

C) Oficina de Control Interno: Hace el seguimiento independiente con periodicidad cuatrimestral o cuando determine necesario, con el fin de presentar informe de aseguramiento de la efectividad del sistema de control

## 7.3. FORMULACIÓN PLAN DE CONTINGENCIA

Es el conjunto de acciones previamente definidas, organizadas y coordinadas que debe ejecutar el proceso durante y después de la materialización de un evento de riesgo, para corregir la materialización del riesgo y minimizar los impactos o efectos negativos que este pueda ocasionar. Los planes de contingencia son dinámicos y cuando se definan deben ser revisados permanentemente para verificar su pertinencia frente al riesgo. con el fin de:

- Garantizar la continuidad de la actividad, función y objetivo del proceso.
- Proteger a las personas, los recursos y la información.
- Disminuir la magnitud del impacto sobre el cumplimiento de la misión institucional.
- Restablecer la operación en el menor tiempo posible.

La Unidad de Gestión General dispone de la estructura del plan de contingencia conforme a lo establecido en el Formato DP-F-009 Matriz de Identificación y Administración de Riesgos, específicamente en la hoja "Plan de Contingencia", la cual se compone de los siguientes elementos:

- ✓ **Descripción del Riesgo**: corresponde al resultado de la identificación del riesgo, una vez aplicada la metodología definida bajo la estructura Posibilidad de + Impacto + Causa inmediata + Causas raíz. Esta información se encuentra consignada en la hoja "gestión" del formato DP-F-009, columna I.
- ✓ **Tipo de Riesgo:** hace referencia a la clasificación del riesgo, conforme a la información registrada en la hoja "gestión" del formato DP-F-009, columna J.
- ✓ **Definición Situación de Materialización de Riesgo:** consiste en identificar, describir y delimitar de manera previa y explícita los escenarios, hechos o circunstancias concretas en los cuales se considera que un riesgo se ha materializado. Estas situaciones deben explicar de forma clara, objetiva y específica la(s) acción(es), evento(s) o condición(es) observable(s) que evidencia que los controles no fueron suficientes para evitar la ocurrencia del riesgo.
- ✓ **Actividades:** refiere a la planificación de acciones correctivas que se deben ejecutarse de manera inmediata ante una materialización de riesgo.
- ✓ **Evidencia de Ejecución de las Acciones:** corresponde a la descripción de los soportes verificables que respaldan la ejecución de las actividades desarrolladas.

*Figura No. 9 Estructura plan de contingencia*


*Fuente: Elaboración propia GVP – Formato DP-F-009 Matriz de Identificación y Administración de Riesgos*

Los riesgos identificados, así como el plan de tratamiento y el plan de contingencia, deben ser socializados de manera periódica al interior de cada proceso por el Gestor Interno de Valor Público, con el propósito de sensibilizar a los equipos de trabajo sobre la oportunidad y efectividad en la implementación de los controles definidos para cada riesgo, así como en la ejecución de las actividades contempladas en el plan de tratamiento, orientadas a prevenir su materialización.

No obstante, en caso de que el evento de materialización del riesgo se presente, resulta fundamental que el equipo de trabajo conozca y comprenda el plan de contingencia, a fin de garantizar la adopción oportuna de las acciones requeridas durante y después de la ocurrencia del evento.

## 7.4. MATERIALIZACIÓN DE RIESGOS

Teniendo en cuenta que en cualquier momento puede materializarse un riesgo, evidenciando que los controles establecidos no fueron suficientes para mitigar su ocurrencia, el líder del proceso, el Gestor Interno de Valor Público y el equipo de trabajo involucrado deberán, en primera instancia, activar y ejecutar el plan de contingencia definido, con el fin de atender de manera inmediata los efectos generados por el evento. Posteriormente se contará con un plazo máximo de 5 días hábiles para notificar mediante comunicado oficial a la Dirección de Planeación y Presupuesto – Grupo de Gestión y Valor Público la materialización del riesgo, así como realizar el registro del evento en la plataforma Suite Visión Empresarial -SVE, módulo de riesgos, realizando un análisis detallado de lo sucedido.

En este sentido, la descripción de la materialización debe ser objetiva, clara y sustentada, dando respuesta, según aplique, a los siguientes interrogantes:

- ¿Que causó la materialización del riesgo?

- ¿Qué control no fue efectivo para evitar la materialización del riesgo?
- ¿Qué impacto genera para el proceso o la institución la materialización de ese riesgo?
- ¿Es posible que se haya presentado en otras ocasiones sin haberlo detectado?
- ¿Qué actividades se deben desarrollar para fortalecer los controles?
- ¿Quiénes están implicados en la materialización del riesgo?

Así mismo, el registro correspondiente deberá realizarse de manera inmediata en la plataforma SVE, una vez se identifique el evento; en consecuencia, los responsables no deberán esperar a los ejercicios periódicos de monitoreo para efectuar el reporte.

Adicionalmente, la dependencia responsable del riesgo, al momento de reportar su materialización, deberá documentar la Acción Correctiva (AC) en la plataforma Suite Visión Empresarial (SVE), en el módulo de Mejoras, en cumplimiento de lo establecido en el procedimiento vigente para el tratamiento de acciones correctivas en la entidad. La denominación de la Acción Correctiva en la SVE deberá seguir la siguiente estructura: **"Tratamiento de Acción Correctiva por Materialización de Riesgos – SGDI"**, con el fin de garantizar su adecuada trazabilidad e identificación.

Se considera importante precisar que, adicional a las situaciones de materialización del riesgo definidas en el plan de contingencia, puede configurarse como un escenario complementario la identificación de eventos de materialización derivados de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD), o de cualquier dependencia que gestione la relación con la ciudadanía, siempre que estos se encuentren directamente asociados a los riesgos del proceso. En estos casos, dicha situación deberá ser entendida como una materialización de riesgo inminente, la cual deberá ser gestionada y tratada conforme a lo establecido en el presente numeral, incluyendo la activación del plan de contingencia, el análisis del evento, el reporte en la plataforma SVE y la implementación de las acciones correctivas correspondientes.

Finalmente, La materialización de un riesgo implica la revisión, actualización y ajuste de la matriz de riesgos del proceso, así como la revisión y fortalecimiento obligatorio del o los controles asociados al evento materializado, con el fin de prevenir su recurrencia y mejorar la efectividad del sistema de control.

## 8. DEFINICIONES

- Gestión del Riesgo: actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de estos de forma que se apoye el cumplimiento de los objetivos de la entidad.
- Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- Análisis de Riesgos: determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

- Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- 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.
- Causa Raíz: causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- Corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Control Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- Control correctivo Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones); está orientado a disminuir el nivel de impacto del riesgo.
- Control preventivo Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones); está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- Corrupción Abuso de posiciones de poder o de confianza, para el beneficio particular en detrimento del interés colectivo, realizado a través de ofrecer o solicitar, entregar o recibir bienes o dinero en especie, en servicios o beneficios, a cambio de acciones, decisiones u omisiones.
- Evento: hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo. Tiene relación directa con las actividades críticas de los planes de acción, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.
- Efecto 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.
- Evaluación del riesgo Etapa que establece el cruce cuantitativo de las calificaciones de probabilidad e impacto, antes y después de controles.
- Factor de Riesgo Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.
- Frecuencia: periodicidad con que ha ocurrido un evento.
- Gestión del riesgo 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.
- Gestor del Riesgo: funcionario líder de la dependencia, quien apoya al responsable del riesgo.
- Gestionar oportunidades: Aprovechar de manera oportuna y adecuada las oportunidades y fortalezas identificadas en el contexto de la organización y las

necesidades de las partes interesadas; para cumplir con los objetivos del proceso y planes estratégicos de la entidad.

- Identificación del Riesgo: consiste en identificar las posibles causas concretas de los riesgos, así como los efectos de su materialización. Lo anterior, requiere un correcto conocimiento de las funciones asignadas a la dependencia, objetivo del proceso y misión de la Entidad, así como el entorno social, político y cultural. De acuerdo con el resultado de lo anterior, se determinará la situación no deseada.
- Impacto Los efectos que puede ocasionar a la organización la materialización del riesgo.
- Líneas de defensa: permiten mejorar las comunicaciones en la gestión del riesgo, mediante la definición de roles, funciones y deberes.
- Mapa de riesgos: documento con la información resultante de la gestión del riesgo.
- Materialización del riesgo Ocurrencia de un riesgo identificado o no identificado de la Entidad.
- MIPG: Modelo Integrado de Gestión y Planeación.
- Monitoreo del riesgo Verificación, supervisión, observación crítica o determinación continúa del estado del riesgo con el fin de identificar cambios del nivel de desempeño requerido o esperado de cada una de las etapas de administración, así como el nivel de cumplimiento y efectividad de los controles y acciones definidas.
- Monitorear: comprobar, inspeccionar, verificar, supervisar, observar o registrar cada uno de los controles definidos para evitar la materialización de los riesgos, con el fin de identificar sus posibles cambios y optimizar las respuestas para la administración del riesgo a través de la mejora continua.
- 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.
- Políticas de manejo del Riesgo: son los lineamientos que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad en función de su evaluación.
- 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.
- Responsable del riesgo: es el encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo para cada uno de los riesgos del proceso bajo su responsabilidad.
- Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- Riesgo Inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- Riesgo residual: 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 de corrupción: posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.
- Tratamiento: Es el proceso para modificar el riesgo, el tratamiento del riesgo puede implicar evitar el riesgo decidiendo no iniciar o continuar la actividad que lo causó, incrementar el riesgo para conseguir una oportunidad, suprimir la fuente del riesgo, cambiar la probabilidad, cambiar los efectos o retener el riesgo mediante una decisión informada. Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.
- Valoración del Riesgo. Etapa que establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa se determina el riesgo residual, la opción de manejo a seguir y si es necesario, las acciones a desarrollar para el fortalecimiento de controles.

## 9. ABREVIATURAS, UNIDADES DE MEDIDA Y EXPRESIONES ACEPTADAS

- UGG: Unidad de Gestión General
- MDN: Ministerio de Defensa Nacional
- PES: Plan Estratégico Sectorial
- PEI: Plan Estratégico Institucional
- SGDI: Sistema de Gestión y Desempeño Institucional
- DAFP: Departamento Administrativo de la Función Pública
- MIPG: Modelo Integrado de Planeación y Gestión
- MOP: Modelo de Operación por Procesos
- COSO: Committee of Sponsoring Organizations of the Treadway Commission (Comité de Organizaciones Patrocinadoras de la Comisión Treadway)
- ERM: Enterprise Risk Management (Gestión de Riesgos Empresariales)
- KRI: Indicador Clave de Riesgo
- KPI: Indicadore clave de proceso
- AC: Acción Correctiva
- OM: Oportunidad de Mejora

## 10. ANEXOS

- Anexo 1. "Herramienta Diagnostico Modelo Madurez UGG"
- Anexo 2." Metodología para la definición del apetito del riesgo".
- Anexo 3 "Metodología General para la Gestión de Riesgos"
- Anexo 4 "Metodología para la gestión de riesgos Fiscales"
- Anexo 5 "Riesgos de Seguridad de la Información"
- Anexo 6 "Sistema de Gestión de Riesgos para la Integridad Pública"
- Anexo 7 "Metodología para la gestión de riesgos de Salud y Seguridad en el Trabajo"
- Formato DP-F-009 Matriz de Identificación y Administración de Riesgos

## 11. REFERERENCIAS BIBLIOGRÁFICAS


- Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025)
- Manual Operativo Manual Operativo del Modelo Integrado de Planeación y Gestión, Versión 6.1
- Plan Estratégico del Sector Defensa y Seguridad (PES)
- Plan Estratégico Institucional (PEI)


| HISTÓRICO DE CAMBIOS | | |
|---|---|---|
| **VERSIÓN No.** | **FECHA DE EMISIÓN** | **CAMBIOS REALIZADOS** |
| 1 | 28/04/2022 | Migración documental por actualización del Modelo de Operación por Procesos. |
| 2 | 07/12/2022 | Inclusión de consideraciones generales para identificar riesgos de corrupción – soborno, precisiones sobre los controles transversales aplicables en todos los procesos de la UGG, lineamientos para diseño de nuevos controles y definiciones asociadas a la gestión de riesgos de soborno |
| 3 | 13/12/2023 | Ajuste del apetito del riesgo de la UGG, inclusión Definición de situaciones de materialización, ajuste a la evaluación de los controles y nuevos pasos para el monitoreo de los riesgos |
| 4 | 01/08/2024 | Ajustes de la forma de monitoreo del riesgo, se incluyó la metodología de Oportunidades de la UGG. |
| 5 | 22/05/2026 | Ajuste metodológico de acuerdo con lineamientos del DAFP:<br>• Alineación estratégica de la gestión del riesgo y el modelo integrado de planeación y gestión MIPG.<br>• Gobernanza de la gestión del riesgo (esquema de líneas de defensa)<br>• Niveles de madurez para la gestión del riesgo<br>• Política para la gestión integral de riesgos<br>• Apetito del riesgo<br>• Gestión del riesgo<br>• Seguimiento, monitoreo y revisión de riesgos |

# ANEXO 1. INSTRUMENTO DE AUTODIAGNÓSTICO PARA DETERMINAR EL NIVEL DE MADUREZ DE LA GESTIÓN INTEGRAL DEL RIESGO

## I.CONTEXTO, ANTECEDENTES Y ASPECTOS GENERALES

Teniendo en cuenta que la gestión integral del riesgo en todas sus fases debe ser un proceso conjunto, permanente e interactivo entre todos los actores institucionales, pero especialmente, entre la línea estrategica, segunda línea en relación con la gestión del riesgo y la tercera línea de defensa, se ha identificado la necesidad de establecer un marco general que le permita a las entidades establecer su estado actual respecto de la gestión integral del riesgo que contribuya a tener un punto de partida objetivo para la toma de decisiones tendientes a la mejora del proceso.

Es así como el Departamento Administrativo de la Funcion Pública ha utilizado un marco de referencia sobre gestión de riesgos ya existente: el Committee of Sponsoring Organizations of the Treadway Commissión -COSO ERM, y a partir de la herramienta desarrollada por The Institute of Internal Auditor - The IIA (España), que utiliza esta estructura para determinar el nivel de madurez de la gestión del riesgo, ha adaptado a las necesidades, terminos y estructura de la gestión del riesgo en el sector público Colombiano para incorporarla como un aspecto de base en la Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas, pues se hace necesario comprender el estado actual en la gestión del riesgo institucional, no solo desde la estructura de la política de administración del riesgo, sino considerando un espectro mas amplio que brinda el COSO ERM y que permitira tener una mayor comprensión respecto de los niveles de implementación de los componentes, principios y resultados en relación con los eventos o materializaciones que han sido evidenciados, información esencial para determinar la efectividad de las actividades de control establecidas por la entidad.

Adicionalmente, como se ha planteado en el numeral 5.2 de la Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces, Versión 3 de Septiembre 2023, especificamente en la tabla 6, las unidades u oficinas de control interno, auditoría interna o quien haga sus veces, con base al nivel de madurez de la gestión del riesgo en la entidad podrán identificar las actividades esperadas a ejecutar en el marco del rol de Evaluación de la Gestión del Riesgo, a fin de que el desarrollo de este rol aporte mayor valor a las tomas de decisiones de la alta dirección.

De esta manera el formato podrá utilizado tanto por las Oficinas de Planeació o la dependencia que haga sus veces para el análisis de la gestión del riesgo institucional, o bien por parte de las unidades u oficinas de control interno o quienes hagan sus veces como insumo para el análisis de priorización basado en riesgos para la formulación de su plan anual de auditoría.

## II.INSTRUCCIONES PARA EL USO DEL INSTRUMENTO DE AUTODIAGNÓSTICO VERSIÓN 1.0.

La ESTRUCTURA del instructivo del Instrumento de Autodiagnóstico para Determinar el Nivel de Madurez de la Gestión del Riesgo-, que en adelante será llamado como Instrumento de Autodiagnóstico del Riesgo, consta de:

→1 hoja de "Instrucciones"
→ 1 hoja que muestra la "*Escala de Madurez* " de referencia.
→ 5 plantillas "*Componente* " para recopilar el nivel de madurez de las características fundamentales de cada uno de los cinco Componentes y de sus Principios (hojas "1. Gobierno y Cultura", "2. Estrategia y Objetivos", , etc.)
→ 1 hoja resumen "*Mapa de Calor* " en la cual se consolidan los resultados de la evaluación de los Componentes y sus Principios y se muestra su representación gráfica en formato de mapa de calor.
→ 1 hoja "*Resumen* " en la cual se consolidan los resultados de la evaluación de los Componentes y sus Principios y se muestra su representación gráfica en formato de gráfico radial.

El diagnóstico consiste en:

→ Responder a cada una de las preguntas, o "*Puntos de Reflexión* ", de cada una de las hojas "*Componente* ".
→Para cada "*Punto de Reflexión* " seleccionar el Grado de Madurez que se correspondería con base en la siguiente escala:

1- Nunca (El punto de reflexión evaluado no se tiene implementado en su elemento basico o aún teniendolo implementado no se operativiza o no se evalúa)
2- Raramente (El punto de reflexión evaluado se tiene implementado con debilidades y no se evalúa)
3- A veces (El punto de reflexión evaluado se tiene implementado con debilidades y se evalúa algunas veces)
4- Frecuentemente (El punto de reflexión evaluado se tiene implementado, operativizado y se evalúa de forma regular)
5- Siempre (El punto de reflexión evaluado se tiene implementado, operativizado y se evalúa siempre)

El Grado de Madurez seleccionado se corresponde con una calificación del 1 al 5, con base en la cual se determina la nota (media aritmética) del Principio y del Componente.

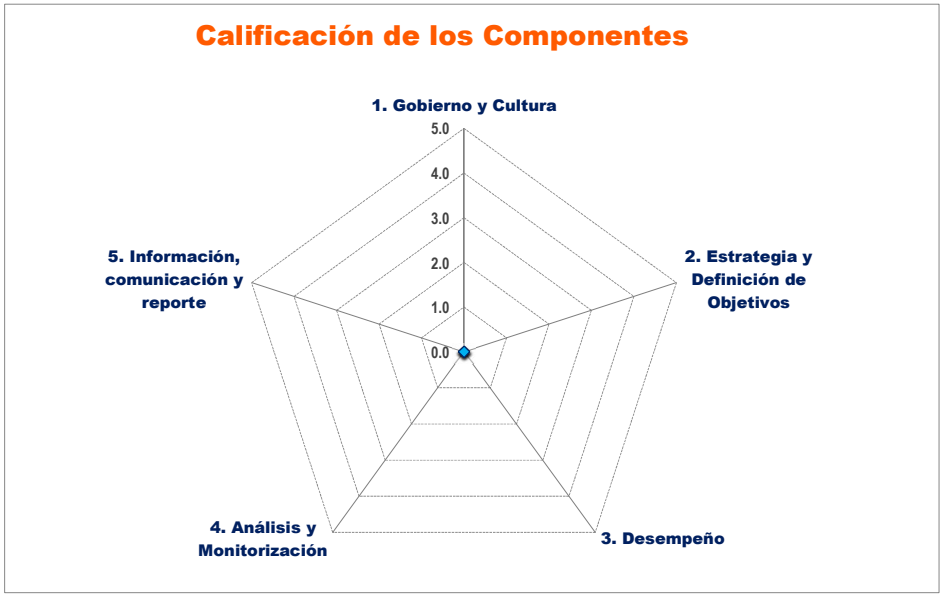
Los resultados se reportan en dos formatos:

### (i) Mapa de Calor

## RESUMEN DE RESULTADOS

| | CALIFICACIÓN | | | | | |
|---|---|---|---|---|---|---|
| | Componente | Principio 1 | Principio 2 | Principio 3 | Principio 4 | Principio 5 |
| 1. Gobierno y Cultura | | | | | | |
| 2. Estrategia y Definición de Objetivos | | | | | | |
| 3. Desempeño | | | | | | |
| 4. Análisis y Monitorización | | | | | | |
| 5. Información, comunicación y reporte | | | | | | |

| | |
|---|---|
| MADUREZ DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DEL RIESGO | |




| Análisis de Resultados |
|---|
| |

| ÍNDICE GENERAL DE MADUREZ DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DEL RIESGO | - | PENDIENTE | | ATENCIÓN MÁXIMA | ATENCIÓN ALTA | ATENCIÓN MEDIA | ATENCIÓN LEVE |
|---|---|---|---|---|---|---|---|
| **1. Gobierno y Cultura** | | | | | | | |
| 1. Supervisión de Riesgos a través del Comité Institucional de Coordinación de Control Interno | | | | | | | |
| 2. Establece Estructuras Operativas | | | | | | | |
| 3. Define la Cultura Deseada | | | | | | | |
| 4. Demuestra Compromiso con los Valores del Servicio Público | | | | | | | |
| 5. Atrae, Desarrolla, y Retiene a Profesionales Capacitados | | | | | | | |
| **2. Estrategia y Definición de Objetivos** | | | | | | | |
| 6. Analiza el Contexto Sectorial/Territorial e Institucional | | | | | | | |
| 7. Define el Apetito al Riesgo | | | | | | | |
| 8. Evalúa Estrategias Alternativas | | | | | | | |
| 9. Formula Objetivos Estrategicos y Operacionales | | | | | | | |
| **3. Desempeño** | | | | | | | |
| 9. Identifica y describe el Riesgo | | | | | | | |
| 10. Evalúa el Riesgo Inherente | | | | | | | |
| 11. Diseña Controles efectivos | | | | | | | |
| 12. Prioriza Riesgos | | | | | | | |
| 13. Desarrolla una visión integral | | | | | | | |
| **4. Análisis y Monitorización** | | | | | | | |
| 14. Evalúa los Cambios Significativos | | | | | | | |
| 15. Revisa el Riesgo y el Desempeño | | | | | | | |
| 16. Persigue la Mejora de la Gestión del Riesgo | | | | | | | |
| **5. Información, comunicación y reporte** | | | | | | | |
| 17. Aprovecha la Información y la Tecnología | | | | | | | |
| 18. Comunica Información sobre Riesgos | | | | | | | |
| 19. Informa sobre el Riesgo, la Cultura y el Desempeño | | | | | | | |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez | Puntuación |
|---|---|---|---|---|
| 1. Gobierno y Cultura | 1. Supervisión de Riesgos a través del Comité Institucional de Coordinación de Control Interno | 1.1. El Reglamento del Comité Institucional de Coordinación de Control Interno o instancia equivalente establece sus competencias en materia de supervisión de gestión de riesgos, de acuerdo al esquema de líneas? | | |
| | | 1.2. Los miembros del Comité Institucional de Coordinación de Control Interno o instancia equivalente realizan por lo menos dos veces al año supervisión sobre la efectividad de la gestión de riesgos? | | |
| | | 1.3. Existe una Política de Administración de Riesgos aprobada por el Comité Institucional de Coordinación de Control Interno, donde se establecen los principales roles, responsabilidades y competencias? | | |
| | | 1.4. La Política de Administración de Riesgos es consistente con otros marcos relacionados (v.g.; seguridad, calidad, financiero, seguridad pacviente, asistenciales, etc.) ? | | |
| | 2. Establece Estructuras Operativas | 2.1. El marco de gestión de riesgos definido a traves de la Politica de Administración de Riesgos ha sido ampliamente comunicado a través de la organización | | |
| | | 2.2. Están claramente establecidos los flujos de aprobación y reporte en la gestión de riesgos? | | |
| | | 2.3. Están claramente identificados las instancias de 1a., 2a y 3a Línea de Defensa en las principales áreas de la entidad? | | |
| | | 2.4. Están claramente identificados los aspectos claves de exitos de 2a Línea, sus funciones de asequramiento y su nivel de confianza? | | |
| | | 2.5. Los responsables de riesgos de los procesos/planes/programas/proyectos rinden informes al Comité Institucional de Coordinación de Control Interno o instancia equivalente sobre el cumplimiento de los objetivos basados en los niveles de exposición a riesgos? | | |
| | 3. Define la Cultura Deseada | 3.1. ¿Se evidencia una cultura orientada a la gestión preventiva del riesgo, promovida desde la Alta Dirección? | | |
| | | 3.2. ¿El riesgo se analiza antes de haber establecido las estrategias o realizado la planificación institucional? | | |
| | | 3.3. ¿Los objetivos de las procesos o de los planes, programas proyectos generan incentivos o presiones que favorecen un comportamiento contrario a los valores del Código de Integridad? | | |
| | | 3.4. La Política de Administración de Riesgos refleja los principios de comportamiento esperados, conforme a lo previsto en el Código de Integridad de la organización? | | |
| | 4. Demuestra Compromiso con los Valores del Servicio Público | 4.1. Se ponen a disposición de los grupos de valor, tanto interno como externo, los valores de la entidad y los diferentes mecanismos utilizados para garantizar su apropiación por parte de los servidores y contratistas? | | |
| | | 4.2. Demuestra la Alta Dirección con su comportamiento su compromiso con los valores del servicio público (tone at the top)? | | |
| | | 4.3. Demuestra la Alta Dirección con su comportamiento su compromiso con la gestión del riesgo institucional (tone at the top)? | | |
| | | 4.4. Los miembros del Comité Institucional de Coordinación de Control Interno o instancia equivalente promueven activamente la cultura de gestión de riesgos entre el personal operativo? | | |
| | | 4.5. El proceso de inducción de nuevos servidores incorpora contenidos orientadores sobre la gestión preventiva de riesgos? | | |
| | | 4.6. Se realizan mediciones / evaluaciones sobre el nivel de cultura de riesgos entre los empleados de forma regular? | | |
| | 5. Atrae, Desarrolla, y Retiene a Profesionales Capacitados | 5.1. El personal de segunda línea respecto de la gestión de riesgos dispone de las competencias, habilidades y conocimiento necesario para realizar sus tareas? | | |
| | | 5.2. Los objetivos del proceso encargado de liderar la gestión de riesgos en la entidad están alineados con los de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas? | | |
| | | 5.3. Existe un plan de gestión del conocimiento para los puestos clave de gestión de riesgos? | | |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez | Puntuación |
|---|---|---|---|---|
| 2. Estrategia y Definición de Objetivos | 6. Analiza el Contexto Sectorial/Territorial e Institucional | 6.1. ¿La entidad ha identificado y definido su contexto externo y la alineación con el plan estrategico sectorial (nación)/plan de desarrollo municipal, distrital o departamenmtal (territorio)? | | |
| | | 6.2. ¿La entidad ha formulado un Plan estratégico institucional aprobado por la Alta Dirección? | | |
| | | 6.3. La Politica de Administración de Riesgos incorpora el análisis de los factores internos y externos que puedan repercutir sobre los objetivos institucionales (estratégicos, de operaciones, etc.)? | | |
| | | 6.4. Se analiza de forma sistemática la información externa para identificar los cambios relevantes en el contexto de la entidad e identificar riesgos emergentes? | | |
| | | 6.5. Se analiza de forma sistemática la información interna para identificar los cambios relevantes en el contexto de la entidad e identificar riesgos emergentes? | | |
| | 7. Define el Apetito al Riesgo | 7.1. Existe una "declaración del apetito al riesgo" adecuadamente formalizada? | | |
| | | 7.2. Es competencia exclusiva del Comité Institucional de Coordinación de Control Interno o instancia equivalente para la gestión integral del riesgo la definición del apetito al riesgo? | | |
| | | 7.3. Se promueve activamente que la Alta Dirección y las instancias clave de 2a línea conozcan el apetito al riesgo de la organización? | | |
| | | 7.4. El apetito al riesgo es considerado en los procesos de toma de decisiones? | | |
| | | 7.5. Se involucra al Comité Institucional de Coordinación de Control Interno o instancia equivalente en la toma de decisiones que pudieran implicar incumplir con el apetito al riesgo establecido? | | |
| | | 7.6. Se monitoriza activamente el cumplimiento con el apetito al riesgo en todos los procesos? | | |
| | 8. Evalúa Estrategias Alternativas | 7.1. La estrategia de la entidad está alineada con su misión, visión y valores? | | |
| | | 7.2. En el proceso de planeación estratégica, se analizan los riesgos y oportunidades aplicando metodologías que permitan contar con datos e información para su mejora? | | |
| | | 7.3. Participan sistemáticamente las instancias clave en la gestión del riesgo en el proceso de planeación estratégica (instancias de 2a línea identificados y la 3a línea? | | |
| | 9. Formula Objetivos Estrategicos y Operacionales | 8.2. La entidad ha definido objetivos estrategicos? | | |
| | | 8.2. Los objetivos estratégicos son desarrollados en objetivos de procesos/planes/programas/proyectos, etc.? | | |
| | | 8.2. Los objetivos tanto estratégicos como operacionales son especificos, medibles, observables, alcanzables y relevantes? | | |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez | Puntuación |
|---|---|---|---|---|
| 3. Desempeño | 9. Identifica y describe el Riesgo | 9.1. Existen procesos para identificar sistemáticamente los riesgos (en todas sus tipologías) que repercuten en la consecución de los objetivos estratégicos y de procesos/planes/programas/proyectos? | | |
| | | 9.2. Se evalúa la identificación de los riesgos (en todas sus tipologías) al menos con carácter anual a fin de identificar posible sub o sobre identificación? | | |
| | | 9.3. Se utiliza la taxonomía de riesgos de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas para catalogar los riesgos por tipología? | | |
| | | 9.4. Para la identificación y descripción de los riesgos (en todas sus tipologías) se realiza el análisis de los factores de riesgo? | | |
| | | 9.5. Para la identificación y decsripción de los riesgos (en todas sus tipologías) se realiza el análisis de los puntos de riesgo? | | |
| | | 9.6. La descripción de los riesgos (en todas sus tipologías) se realiza conforme las estructuras definidas en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas para cada de estas. | | |
| | 10. Evalúa el Riesgo Inherente | 10.1. Se evalúa la probabilidad e impacto de los riesgos identificados (en todas sus tipologías) con base a las escalas y niveles definidos en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas para cada una de las tipologías? | | |
| | | 10.2. Se cuantifica el impacto económico de los riesgos sobre los que se ha identificado un potencial de afectación economica? | | |
| | | 10.3. Se considera el impacto reputacional de los riesgos sobre los que se ha identificado un potencial de afectación reputacional? | | |
| | | Se realiza el análisis de severidad del inherente en el mapa de calor? | | |
| | 11. Diseña Controles efectivos | 11.1. En la descripción de los controles se muestra el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se muestra el sistema que realiza la actividad? | | |
| | | 11.2. En la descripción de los controles se muestra el verbo en el cual se identifica la acción de control a realizar como parte del control (verificar, validar, cotejar, comparar)? | | |
| | | 11.3. En la descripción de los controles se muestra la frecuencia (semanal, mensual, bimestral, trimetsral, semestral o a demanda) de ejecución del control? | | |
| | | 11.4. En la descripción de los controles se muestra el objetivo de la ejecución de este? | | |
| | | 11.5. En la descripción de los controles se definen las fuentes de información (confiables) para la ejecución de este? | | |
| | | 11.6. En la descripción de los controles se muestra la evidencia que permita realizar la trazabilidad a la ejecución de este? | | |
| | | 11.7. Los controles se encuentran documentados en un procedimiento, manual, guía o instructivo que garantice su operativización? | | |
| | 12. Prioriza Riesgos | 12.1. Los riesgos se priorizan con base a su probabilidad e impacto residual? | | |
| | | 12.2. Los riesgos se representan en un mapa de riesgos y de matriz de calor que facilita su priorización? | | |
| | | 12.3. Se asigna un área, personal responsable y fechas de ejecución para monitorear los riesgos críticos identificados? | | |
| | 13. Desarrolla una visión integral | 13.1. Existe un registro/inventario de riesgos centralizado a nivel de proceso, plan, programa, proyecto? | | |
| | | 13.2. Se analizan las posibles interdependencias entre los riesgos identificados en cada proceso, plan, programa, proyectos para obtener una visión integral de la operación y la gestión del riesgo? | | |
| | | 13.3. Existe un registro/ inventario de riesgos centralizado para un análisis integral sobre la efectividad de la gestión del riesgo? | | |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez | Puntuación |
|---|---|---|---|---|
| 4. Análisis y Monitorización | 14. Evalúa los Cambios Significativos | 14.1. Existe un proceso o esquema que permita monitorear periódicamente los cambios del contexto institucional (i.e.; los factores internos y externos) con posible impacto en la consecución de los objetivos? | | |
| | | 14.2. Se actualiza periódicamente el registro/inventario de riesgos de la organización, incorporando temas emergentes o cambios en el contexto institucional? | | |
| | | 14.3. El Comité Institucional de Coordinación de Control Interno evalúa por lo menos una (1) vez al año la Politica de Administración de Riesgos respecto de:<br><br>1. La adecuación de esta con los requerimientos técnicos,<br>2. la adecuada operativización de esta a través de las primeras líneas de defensa considerando las disposiciones de esta. | | |
| | 15. Revisa el Riesgo y el Desempeño | 15.1. La organización realiza un seguimiento periódico del grado de desempeño para los principales objetivos establecidos | | |
| | | 15.2. Se utilizan métricas de monitorización del riesgo (Key Risk Indicators o KRIs) para alertar respecto de riesgos crecientes o emergentes ? | | |
| | 16. Persigue la Mejora de la Gestión del Riesgo | 16.1. La organización revisa la idoneidad y actualiza su Politica de Administración de Riesgos periódicamente ? | | |
| | | 16.2. Se han implantado mejoras significativas en el proceso de gestión de riesgos en el último año? | | |

| Componente | Principio | Puntos de Reflexión | Grado de Madurez | Puntuación |
|---|---|---|---|---|
| **5. Información, comunicación y reporte** | **17. Aprovecha la Información y la Tecnología** | 17.1. Los miembros del Comité Institucional de Coordinación de Control Interno o instancia esquivalente tienen acceso directo a la Información de riesgos que necesitan para cumplir con sus responsabilidades de supervisión | | |
| | | 17.2. Se dispone de una herramienta informática o algún otro mecanismo que centralice la gestión del riesgo? | | |
| | | 17.3. Las instancias de 1a. y 2a. Línea de Defensa tienen acceso directo a la herramienta para la carga, análisis y reporte de los riesgos bajo su responsabilidad? | | |
| | **18. Comunica Información sobre Riesgos** | 18.1. Están claramente establecidos los flujos de aprobación y reporte de la información en materia de riesgos? | | |
| | **19. Informa sobre el Riesgo, la Cultura y el Desempeño** | 19.1. Existen procesos de reporte estandarizado a los diferentes niveles organizacionales? | | |
| | | 19.2. Se generan reportes cualitativos (tendencia histórica, perspectiva futura, nivel de aseguramiento, etc.) como cuantitativos (nivel de exposición, nivel máximo, etc.) de los principales riesgos? | | |
| | | 19.3. Se reportan los riesgos materializados y su impacto real sobre los objetivos de la entidad? | | |
| | | 19.4. Se reporta sobre la cultura de riesgos? | | |

Defensa

**ANEXO 2**
**METODOLOGIA PARA LA DEFINICIÓN DEL APETITO DEL RIESGO EN LA UNIDAD DE GESTIÓN GENERAL - UGG**

| | |
|---|---|
| **1. Alinear el apetito con los objetivos institucionales.**<br><br>Vinculación con la planeación institucional o compromete el cumplimiento de uno o varios objetivos estratégicos definidos en el Plan Estratégico Institucional, así como de los objetivos de proceso establecidos en el Modelo de Operación por Procesos de la entidad. | |
| **2. Categorizar los Tipos de Riesgo**<br><br>Se agrupan los riesgos para darles un tratamiento diferenciado, de acuerdo con su naturaleza y sistema de gestión vigente en la UGG. | |
| **3. Definir la Capacidad de Riesgo**<br>Es el límite máximo de pérdida o impacto que la Unidad de Gestión General del Ministerio de Defensa puede soportar antes de entrar en crisis técnica o financiera. | |
| **4. Determinar los Niveles de Apetito (Escalas)**<br>se debe determinar Escalas: cero, baja, moderada, alta y extrema. | |
| **5. Riesgos de tolerancia cero:** de acuerdo con el enfoque integral permite identificar aquellos riesgos frente a los cuales la entidad adopta una posición de tolerancia cero. | |
| **6. Establecer Tolerancias**<br>La tolerancia es el limite o la desviación aceptable frente al apetito definido.<br>Acción: Definir indicadores . Si un indicador supera el nivel de apetito, se deben activar planes de respuesta inmediato.<br>A partir de de las métricas del apetito del riesgo, se recomienda la inclusión de límites e indicadores de riesgo. | |
| **7. Redactar la Declaración de Apetito de Riesgo**<br>Establecer el Marco de Apetito de Riesgo de la Unidad de Gestión General del Ministerio de Defensa Nacional (UGG-MDN), el cual será sometido a validación y aprobación por parte del Subcomité de Control Interno. | |
| **8. Monitoreo y Revisión Continua**<br>El apetito no es estático; cambia con el entorno de seguridad del país o cambios en el Gobierno. | |

# *ANEXO 3*

# *"METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS"*

La aplicación de la presente metodología será considerada para la estructuración de la tipología de riesgos gestionados y administrados por la Unidad de Gestión General del Ministerio de Defensa Nacional. Lo anterior, en concordancia con la estructura metodológica definida para cada riesgo, garantizando su adecuada identificación, análisis y tratamiento, sin que ello implique desconocer o contradecir el tipo de riesgo y/o el sistema de gestión al cual se encuentre asociado.

## RIESGOS OPERATIVOS Y/O DE GESTIÓN

Refiere a la identificación y tratamiento de los riesgos asociados a la operación de la entidad, en otras palabras, corresponden a los riesgos asociados al funcionamiento interno y a la gestión operativa de la entidad, derivados de la posibilidad de fallas o deficiencias en los procesos, procedimientos, sistemas de información, infraestructura, talento humano, estructura organizacional o en la articulación y coordinación entre dependencias. Estos riesgos pueden afectar el cumplimiento de los objetivos estratégicos, así como la continuidad operativa, la eficiencia administrativa, la calidad de los bienes y servicios entregados y la generación de valor público. Su gestión es transversal a todos los procesos y niveles de la entidad.

De acuerdo con lo anterior los pasos determinados por la Unidad de Gestión General del Ministerio de Defensa para la gestión integral de riesgos Operativos y/o de Gestión será la descrita a continuación:

## PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

**1.1. Identificación de los riesgos:** debe realizarse de manera sistemática, asertiva y precisa, enfocándose en aquellos eventos que puedan generar impactos significativos sobre el cumplimiento de la misión institucional, el logro de los objetivos estratégicos y la adecuada provisión de bienes y servicios. Lo anterior, en coherencia con la Política de Gestión del Riesgo, considerando las necesidades y expectativas de los grupos de valor e interés de la entidad, con el fin de fortalecer la toma de decisiones y la gestión institucional orientada a resultados.

Se establecen como fuentes para la identificación de riesgo los siguientes ítems:

a) **Misión de la Entidad**: Los procesos que, de acuerdo con sus funciones, incidan de manera directa en el cumplimiento de la misión institucional vigente deberán identificar obligatoriamente uno o más riesgos, con el propósito de gestionarlos de forma preventiva y evitar su materialización, en concordancia con el apetito de riesgo definido por la entidad. En este sentido, y conforme con lo establecido en la Resolución 0545 del 20 de febrero de 2025, mediante la cual se adopta el Modelo de Operación por Procesos de la Unidad de Gestión General (UGG), los procesos que contribuyen directamente al cumplimiento de la misión institucional corresponden a los procesos misionales. Estos están conformados por los procesos de Defensa y Seguridad; Gestión de Capacidades e Innovación de la Fuerza Pública; Desarrollo Humano de la Fuerza Pública; Derechos Humanos, Derecho Internacional Humanitario (DIH) y Paz; así como Bienestar y Salud de la Fuerza Pública, los cuales, por su naturaleza estratégica, requieren una gestión del riesgo permanente, integral y articulada con los Objetivos Estratégicos Institucionales.

   Para los riesgos identificados por misionalidad deberán ser registrados con la palabra misional entre paréntesis y resaltado en negrita al final de su nombre "**(MISIONAL)**", con el fin de ser plenamente identificados por los entes de control internos y/o externos que disponga la entidad.

b) **Funciones de las dependencias que conforman el proceso**: Comprende la estructura organizacional de la Unidad de Gestión General y la asignación de roles y responsabilidades, conforme a las funciones establecidas en el Decreto 1874 del 30 de diciembre de 2021. A partir de dichas funciones, los procesos deberán identificar riesgos asociados al cumplimiento de sus funciones y a la adecuada ejecución de sus actividades.

c) **Objetivo del proceso:** Los riesgos deben identificarse teniendo como referencia el objetivo del proceso, descrito en la caracterización del proceso, evaluando aquellos eventos que puedan afectar su cumplimiento, su alineación con los objetivos estratégicos institucionales y su contribución a la generación de valor público, de conformidad con los lineamientos del MIPG.

d) **Contexto interno y externo de la entidad (debilidades y amenazas):** La identificación de riesgos deberá considerar el análisis del contexto interno y externo, particularmente las debilidades y amenazas identificadas, tales como capacidades institucionales, recursos disponibles, cambios normativos, factores sociales, tecnológicos, económicos y ambientales, entre otros, que puedan incidir negativamente en la gestión y en el desempeño del proceso.

e) **Salida No conforme Identificado:** Se deberán identificar riesgos a partir de los servicios no conformes detectados en el marco del Sistema de Gestión y Desempeño Institucional, los cuales evidencian desviaciones frente a los requisitos de los productos, bienes y servicios establecidos por cada proceso y pueden generar impactos sobre la satisfacción de los grupos de valor, la eficiencia operativa y la imagen institucional.

f) **Peticiones, Quejas, Reclamos, Sugerencias, Denuncias (PQRSD):** Las PQRSD constituyen una fuente relevante para la identificación de riesgos, en tanto permiten reconocer fallas recurrentes, debilidades en la prestación de los servicios y situaciones que puedan afectar la transparencia, legalidad, confianza, percepción y satisfacción de los grupos de valor e interés de la entidad.

g) **Nivel de madurez del riesgo:** La identificación de riesgos deberá considerar el nivel de madurez del riesgo en la entidad, entendiendo este como el grado de desarrollo, estandarización, control y mejora continua de las actividades, especialmente para aquellos procesos que se encuentren vinculados de forma directa en el plan de intervención planificado por la entidad, lo cual debe ser analizado de manera integral por cada proceso.

*h)* **Cadena de valor del proceso:** La identificación de riesgos deberá considerar la cadena de valor del proceso, evaluando los riesgos asociados a cada una de sus actividades, interacciones y puntos críticos, así como su impacto en los resultados, productos y servicios entregados a los grupos de valor e interés, definida en la caracterización del proceso, *la cual consiste en un aserie de insumos, actividades de transformación o procesos para la generación de una serie de productos y servicios o resultados orientados a la satisfacción de necesidades y requerimientos de sus grupos de valor que fueron definidos previamente y en sí mismos constituyen una cadena de entrega a través de la cual se produce la transformación*

*necesaria para la producción de productos y servicios (Función Pública, Guía para la gestión por procesos en el marco del MIPG,2020, p.60)*

*Tabla No.1. Alineación cadena de Valor con Caracterización de proceso*


| Insumos | Procesos | Productos | Resultados | Impactos |
|---|---|---|---|---|
| Refiere a los recursos financieros, humanos y materiales empleados para generar los productos. | Actividades realizadas para transformar los insumos en productos | Bienes y servicios elaborados que requieren la población para satisfacer una demanda o dar una respuesta a las causas concretas de un problema | Cambios en el comportamiento o en el estado de los beneficiarios como consecuencia de recibir los productos | Cambios en las condiciones de vida de la población objeto, mayor valor público en términos de bienestar, prosperidad y calidad de vida |
| Alineación con Caracterización de proceso:<br>• Columna de proveedores: conformada por Usuarios y Otras Partes Interesadas Externas / Interno (Proceso)<br>• Columna de Entradas | Alineación con Caracterización de proceso:<br>• Columna de actividades | Alineación con Caracterización de proceso:<br>• Columna de salidas | Refiere a efectos directos y medibles generados a partir del uso de los productos y servicios entregados por la Unidad de Gestión General. Los resultados reflejan cambios en el desempeño institucional, en los procesos, en las capacidades o en la situación de los grupos de valor, y permiten evaluar la efectividad de la gestión pública en el corto y mediano plazo | Refiere a los cambios sostenibles y de largo plazo generados en las condiciones de vida, el bienestar, el ejercicio de derechos y la confianza de la ciudadanía y los grupos de valor, como resultado de la gestión pública desarrollada por la Unidad de Gestión General |

*Fuente: Grupo de Gestión y Valor Público*

**Consideración del cambio climático en la gestión del riesgo**

Adicionalmente, el proceso deberá considerar el cambio climático como una fuente de riesgo de carácter transversal, en el marco del análisis del contexto (interno / externo) y la identificación de riesgos, en concordancia con los lineamientos de la norma ISO 9001 y el enfoque de gestión del riesgo.

Lo anterior, teniendo en cuenta que el cambio climático puede impactar directamente en el cumplimiento de la misión institucional de la entidad, particularmente en aspectos como la continuidad operativa, la infraestructura, la disponibilidad de recursos y las condiciones de operación.

En este sentido, la incorporación del cambio climático en la gestión del riesgo permite fortalecer la identificación de riesgos externos, así como el diseño e implementación de controles preventivos orientados a la anticipación de eventos. De igual manera, contribuye al fortalecimiento organizacional, facilitando la adopción de medidas que permitan a la entidad adaptarse y garantizar la prestación efectiva de sus servicios ante escenarios climáticos adversos.

**1.2. Identificación de áreas de impacto:** corresponde a la determinación de las consecuencias que podría enfrentar la entidad en caso de materializarse un riesgo, considerando los efectos adversos sobre el logro de los objetivos institucionales. Estas consecuencias pueden manifestarse principalmente en dos áreas: *impacto económico o presupuestal*, asociado a pérdidas financieras, sobrecostos, afectación en la ejecución de recursos o limitaciones en la sostenibilidad fiscal; e *impacto reputacional,* relacionado con la pérdida de credibilidad, confianza institucional, imagen pública y legitimidad ante los grupos de valor y partes interesadas. económica (o presupuestal) y reputacional.

**1.3. Identificación de áreas de factores de riesgo:** De acuerdo con la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del DAFP, los factores de riesgo corresponden a las fuentes o condiciones que incrementan la probabilidad de ocurrencia de un evento de riesgo y, por ende, el nivel de exposición de la entidad frente al mismo. Estos factores se derivan del análisis del contexto interno y externo determinado por la entidad asociados a aspectos relacionados con talento humano, tecnología, normatividad, entorno social, económico, político, ambiental, entre otros.

Los factores de riesgo pueden ser de origen interno o externo y, si bien no constituyen causas directas del riesgo, contribuyen a su generación o

potenciación, al crear condiciones que facilitan su materialización. La adecuada identificación de estos factores permite fortalecer el análisis del riesgo inherente y constituye un insumo clave para el diseño de controles y la definición de acciones de tratamiento.

La Función Pública establece un listado con los factores de riesgo que pueden incidir en un proceso, los cuales fueron adecuados de acuerdo con las características propias de la Unidad de Gestión General como se muestra a continuación:

*Tabla No. 2: Factores de Riesgo*

| 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 entidad. | Falta de aplicación de los procedimientos |
| | | Falta segregación de funciones |
| | | 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 grupo de valor o usuario (interno o externo), 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 de los servidores | Fraude Interno |
| | | Soborno |
| | | Gestión inadecuada de conflicto de Intereses |
| | | Corrupción |

| Factor | Definición | Descriptores |
|---|---|---|
| | públicos que afectan la Integridad Pública. | Hurto de activos |
| Infraestructura | Eventos relacionados con la infraestructura física de la entidad. | Daños a activos fijos |
| | | Incendios |
| | | Inundaciones |
| Evento externo | Eventos por situaciones externas que afectan la entidad | Fraude Externo |
| | | Suplantación de identidad |
| | | Atentados, vandalismo, orden público |
| 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 |
| | | Obsolescencia tecnológica |
| Presupuestal | Eventos relacionados con la gestión presupuestal de la entidad | Errores en la programación presupuestal |
| | | Errores en la ejecución presupuestal |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública, p. 51 – Grupo de Gestión y Valor Público*

## 1.4. Causas asociadas a los Riesgo:

De acuerdo con la metodología descrita en la Guía para gestión integral del riesgo en entidades públicas (V7), la identificación de las causas en la gestión del riesgo es un elemento fundamental, toda vez que permite comprender de manera estructural el origen del riesgo, a partir de lo anterior, su importancia se puede resumir en los siguientes aspectos clave:

- Permite entender el "por qué" del riesgo
- Facilita el diseño de controles efectivos
- Reduce la probabilidad de materialización del riesgo
- Mejora la calidad del análisis y tratamiento del riesgo
- Fortalece la mejora continua

Con base en lo anterior es importante identificar las sientes causas.

**a) Causa inmediata:** corresponde a las circunstancias o situaciones más evidentes bajo las cuales se presenta un riesgo; no obstante, estas no constituyen la causa principal o estructural que origina su ocurrencia.

Es decir, corresponde a la condición visible, específica y observable en la que se materializa o podría materializarse un riesgo, y que permite describir de manera concreta el contexto en el cual ocurre el evento. Para su adecuada identificación, debe enfocarse en responder al "cómo se presenta el riesgo", describiendo la situación operativa real (por ejemplo, retrasos, omisiones, incumplimientos, fallas en actividades o en la ejecución de tareas), sin profundizar aún en las razones estructurales que lo originan.

En este sentido, la causa inmediata facilita reconocer señales o manifestaciones evidentes del riesgo dentro del proceso, constituyéndose en un punto de partida para posteriormente identificar la causa raíz.

**b) Causas Identificadas:** corresponden al conjunto de factores intermedios que se determinan a partir del análisis sistemático de la causa inmediata, mediante herramientas como la metodología de los 5 porqués, con el propósito de profundizar en la comprensión del riesgo y establecer la cadena causal que conduce a su origen.
Estas causas reflejan las condiciones, debilidades o fallas progresivas en el proceso (organizacionales, operativas, normativas, tecnológicas o humanas) que, en conjunto, explican cómo se conforma la causa raíz.

En este sentido, permiten transitar desde la manifestación visible del riesgo (causa inmediata) hasta la identificación de la causa estructural (causa raíz), facilitando un análisis más robusto y la definición de controles y acciones correctivas más efectivos.

**c) Causa Raiz:** La causa raíz corresponde a la causa principal o estructural que origina un riesgo, es decir, el factor determinante (acción u omisión) que explica por qué ocurre el evento no deseado. Se caracteriza por mantener una relación directa de causa–efecto con la materialización del riesgo y constituye el origen que, al ser intervenido mediante controles o acciones correctivas, permite prevenir su recurrencia. Su identificación se logra a partir del análisis sistemático de las causas mediante metodologías como los 5 porqués.

Ejemplo:

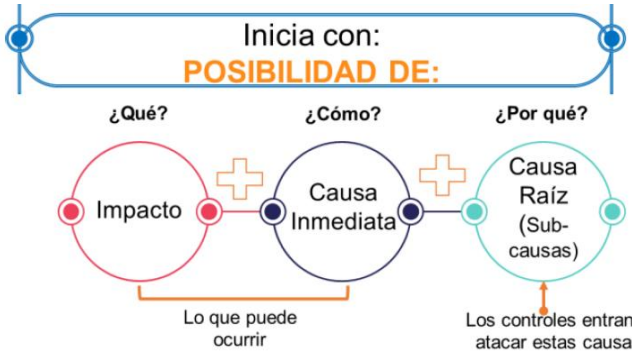
| Causa inmediata (¿cómo se presenta el riesgo?) | Causas Identificadas (Análisis de "5 porqués") | Causa raíz (¿por qué ocurre realmente el riesgo?) |
|---|---|---|
| Registro tardío de las PQRSD en el sistema de gestión, lo que genera retrasos en la asignación y respuesta de las solicitudes. | 1. ¿Por qué hay registro tardío de las PQRSD?<br>Porque las solicitudes no se cargan oportunamente en el sistema por parte de los responsables.<br><br>2. ¿Por qué no se cargan oportunamente?<br>Porque no existe un control que verifique el registro en tiempo real de las solicitudes recibidas.<br><br>3. ¿Por qué no existe ese control?<br>Porque el procedimiento no define claramente puntos de control ni responsables para el registro inmediato.<br><br>4. ¿Por qué el procedimiento no define controles ni responsables?<br>Porque no ha sido actualizado conforme a los lineamientos vigentes de atención al ciudadano y gestión de riesgos.<br><br>5. ¿Por qué no se ha actualizado el procedimiento?<br>Porque no se cuenta con un mecanismo formal de revisión periódica de los procedimientos del proceso. | Ausencia de un mecanismo estructurado de revisión y actualización periódica de los procedimientos del proceso, que garantice la definición clara de controles, tiempos y responsables para la gestión oportuna de las PQRSD |

## 1.5. Descripción del Riesgo:

A partir de la(s) área(s) de impacto, el(los) factor(es) de riesgo, la causa inmediata, al menos dos causas asociadas y la causa raíz identificados, se debe proceder con la formulación de la descripción del riesgo.

En este sentido, la Unidad de Gestión General del Ministerio de Defensa Nacional – UGG establece la siguiente estructura para la denominación de los riesgos, tomando como referencia la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, de la Función Pública, así:

*Figura No. 1: Estructura para la redacción del riesgo*




| Impacto | Causa Inmediata | Causa Raiz |
|---|---|---|
| *Las consecuencias que puede ocasionar a la organización la materialización del riesgo.* | *circunstancias o **situaciones más evidentes** sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.*<br><br>*Características clave: Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.* | *Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles.*<br><br>*Las características clave: Identificar causas raíz y condiciones contribuyentes que pueden clasificarse en: humanas, tecnológicas, normativas, ambientales, organizacionales. Un adecuado análisis de causa raíz debe permitir diferenciar la causa raíz, de la causa inmediata, entendida esta última como las circunstancias más evidentes sobre las cuales se presenta el riesgo y que en ocasiones, no constituyen la causa principal del riesgo.* |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública, p.54*

Ejemplos:

- Posibilidad de afectación reputacional para la entidad, debido al incumplimiento en los plazos establecidos para la formulación y seguimiento de los planes institucionales, como consecuencia de la entrega tardía de información por parte de los procesos, originada en la falta de definición clara de responsables y de un procedimiento estandarizado para el seguimiento a los compromisos institucionales.
- Posibilidad de afectación económica y reputacional para la entidad, por incumplimientos a la gestión documental, como consecuencia de la perdida de expedientes del archivo central.

- Posibilidad de afectación económica para la entidad, derivada de retrasos en la ejecución de los procesos contractuales, debido a errores u omisiones en la elaboración de los estudios previos, causados por debilidades en la capacitación del personal y en la apropiación de los lineamientos normativos y procedimentales aplicables.

## PASO 2: ANÁLISIS DE RIESGO INHERENTE - ANTES DE LA APLICACIÓN DE CONTROLES

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE). Es decir, el estado del riesgo en un escenario sin controles.

A continuación, se explica la probabilidad y el impacto del riesgo, que se debe establecer en esta etapa de análisis (riesgo inherente) y en el riesgo residual (después de la aplicación de los controles).

### 1.6. Determinar la probabilidad

En esta etapa se determina la probabilidad de ocurrencia del riesgo, entendida como la posibilidad de que el evento identificado se materialice, de acuerdo con las condiciones actuales del proceso. La probabilidad se establece en términos de frecuencia o factibilidad, según aplique, y se orienta a identificar el nivel de exposición del proceso al riesgo.

La frecuencia corresponde al número de veces que, durante un período determinado —generalmente un año—, el proceso transita por el punto de riesgo, es decir, cada ocasión en la que se ejecuta la actividad susceptible de verse afectada por la materialización del riesgo. En este sentido, la probabilidad inherente se define como el número de exposiciones al riesgo en dicho período, permitiendo estimar cuántas veces la actividad podría verse impactada, considerando las condiciones actuales del proceso, sin tener en cuenta la efectividad de los controles.

Para valorar la probabilidad de ocurrencia se utilizan los siguientes criterios:

*Tabla No. 3. Criterios para definir el nivel de probabilidad*

| Nivel | Concepto | Frecuencia de la actividad | Probabilidad |
|---|---|---|---|
| 1 | Muy baja | La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año. | 20% |
| 2 | Baja | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año. | 40% |
| 3 | Media | La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año | 60% |
| 4 | Alta | La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5.000 veces por año. | 80% |
| 5 | Muy alta | La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año. | 100% |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública, p.58*

## 1.7. Determinar el impacto

Corresponde a las consecuencias que la Entidad puede enfrentar como resultado de la materialización de un riesgo. Para la construcción de la tabla de criterios se consideran como variables principales los impactos económicos y reputacionales. El impacto debe analizarse y calificarse con base en las consecuencias o efectos identificados durante la fase de descripción del riesgo.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se deberá tomar el nivel más alto.

*Tabla No. 4. Criterios para definir el nivel de impacto*

| Nivel | Nivel de Impacto | Afectación económica | Afectación Reputacional |
|---|---|---|---|
| 1 | Leve – 20% | Afectación menor a 10 SMLMV | El riesgo afecta la imagen de algún área de la UGG. |
| 2 | Menor – 40% | Mayor a 10 SMLMV y menor a 50 SMLMV | El riesgo afecta la imagen de la UGG a nivel interno de conocimiento general de las dependencias, procesos, Alta Dirección y/o de proveedores. |

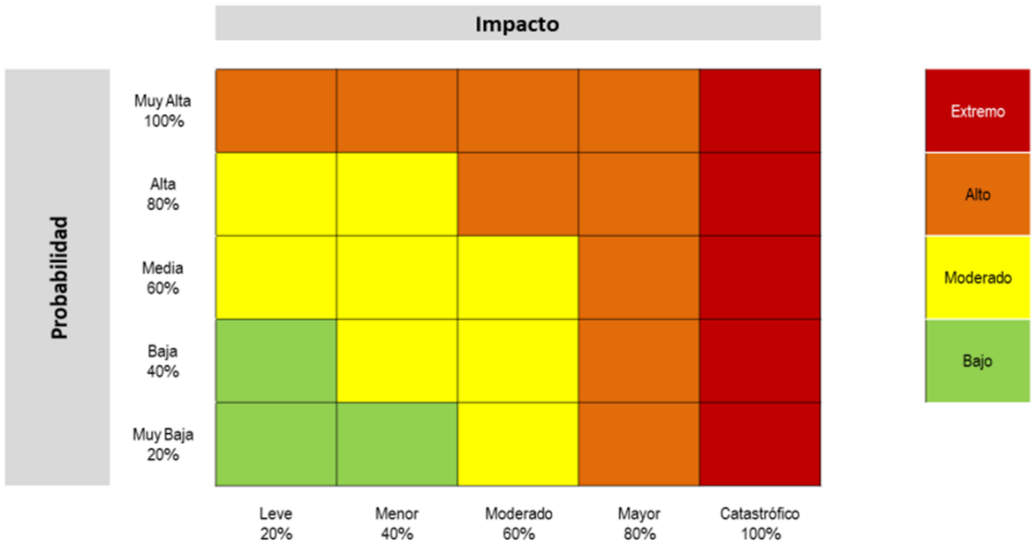
| Nivel | Nivel de Impacto | Afectación económica | Afectación Reputacional |
|---|---|---|---|
| 3 | Moderado – 60% | Mayor a 50 SMLMV y menor a 100 SMLMV | El riesgo afecta la imagen de la UGG con algunos usuarios de relevancia frente al logro de los objetivos. |
| 4 | Mayor – 80% | Mayor a 100 SMLMV y Menor a 500 SMLMV | El riesgo afecta la imagen de la UGG con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o territorial. |
| 5 | Catastrófico – 100% | Mayor a 500 SMLMV | El riesgo afecta la imagen de la UGG. a nivel nacional, con efecto publicitario sostenido a nivel país |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública, p.59*

## 1.8. Análisis de Severidad - Calificación del Riesgo Inherente (Antes de Controles)

Esta se logra a través de la combinación de la probabilidad y el impacto que pueda causar la materialización del riesgo, se definen 4 zonas de severidad en la matriz de calor (Extremo, alto, moderado y bajo) de acuerdo con la siguiente figura:

*Figura No. 2: Matriz de Calor (niveles de severidad del riesgo)*




*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública, p.60*

**PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES**

Conceptualmente, un control se define como la medida diseñada para reducir o mitigar un riesgo, mediante la ejecución de acciones concretas y verificables, dotadas de atributos específicos. Estos controles se establecen a través de políticas, procedimientos u otros documentos institucionales y se implementan con el propósito de proporcionar una seguridad razonable respecto al logro de los objetivos institucionales y al adecuado funcionamiento de los procesos.

Para establecer los controles se debe tener en cuenta:

- La identificación de controles debe realizarse para cada riesgo, a partir de ejercicios de análisis desarrollados mediante entrevistas y mesas de trabajo con los líderes de proceso o con servidores que cuenten con conocimiento experto sobre las actividades a su cargo.

- Analizar los pasos, actividades o etapas de los procesos y procedimientos con el fin de identificar puntos de control existentes o potenciales que puedan incorporarse como controles de gestión del riesgo.

- Para cada riesgo se deberán establecer, como mínimo, tres (3) controles, los cuales deben garantizar la cobertura total de las causas identificadas en la definición del riesgo. Un mismo control podrá atender una o varias causas, siempre que su diseño y alcance lo permitan.

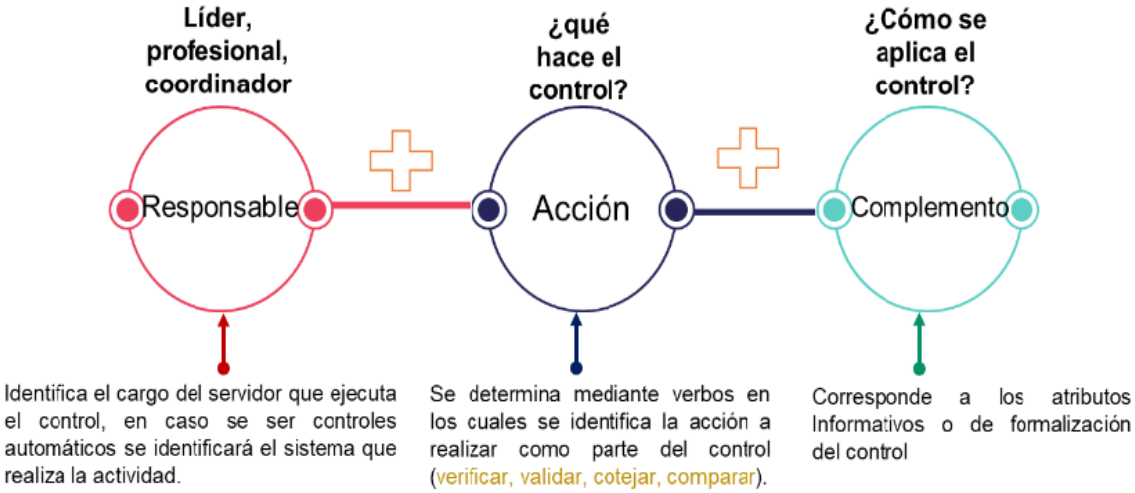
- Los controles deberán encontrarse debidamente documentados y, durante las actividades de monitoreo y seguimiento, será obligatorio adjuntar las evidencias que demuestren su ejecución efectiva, conforme a los criterios definidos por la Entidad

## 1.9. Estructura para describir un control

Para un adecuado diseño de las actividades de un control de acuerdo con lo emitido por la función Pública en la Guía para la gestión integral del riesgo en entidades públicas, versión 7, se propone una estructura para la redacción que agrupa los atributos necesarios para garantizar su

implementación de forma efectiva por parte del responsable, de acuerdo con la siguiente figura:

*Figura No. 3: Estructura para la redacción de controles*




*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública, p.60*

Desglosando la estructura propuesta por la Función Pública, la Unidad de Gestión General del Ministerio de Defensa Nacional, debe incorporar de forma obligatoria los siguientes atributos para la redacción de los controles, con el fin de garantizar la efectividad de estos, así:

- **Responsable**: determine el cargo del responsable que ejecuta el control, es decir es quien en ejecuta el control entre ellos Directores, Coordinadores, Servidores públicos, Gerentes de Proyecto, en caso de que sean controles automáticos se identificará el sistema o aplicativo informático que realiza la actividad.

- **Acción:** Se determina mediante verbos que indican la acción que deben realizar como parte del control.

- **Complemento:** Corresponde a los detalles (atributos del control) que permiten identificar claramente el objeto del control, estos son:

  - ✓ **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.
- ✓ **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.

**Ejemplo de redacción de control:**

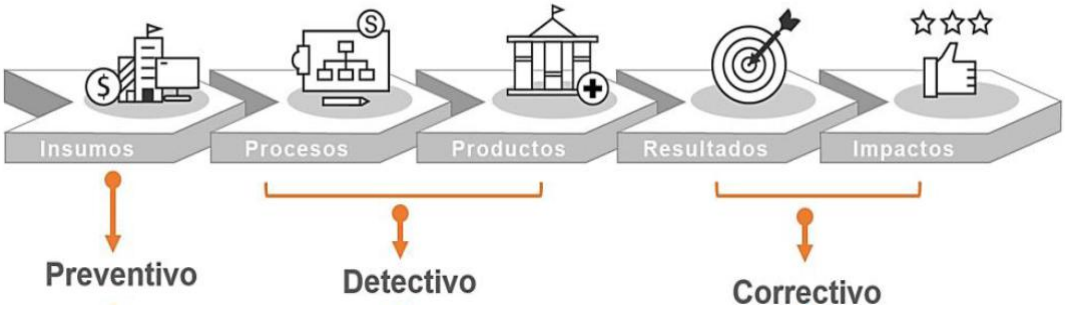
| | |
|---|---|
| **Responsable:** | Director de Finanzas |
| **Acción:** | Revisar. |
| **Complemento:** | Revisar mensualmente la ejecución presupuestal del proceso, comparando los valores comprometidos, obligados y pagados frente al presupuesto aprobado, de conformidad con el **procedimiento** de seguimiento presupuestal. La **frecuencia** del control será mensual. La **evidencia** corresponde a los informes de ejecución presupuestal generados y firmados, así como a los reportes del sistema financiero institucional. La **ejecución** se realiza con base en información extraída de fuentes oficiales y confiables; cuando se detectan desviaciones relevantes, se definen y comunican las acciones correctivas correspondientes para su implementación. |

## 1.10. Tipologías de controles

La activación de un control puede generarse en las distintas etapas del ciclo de los procesos y se evidencia a través de la ejecución de la cadena de valor definida por cada uno de ellos. Este ejercicio permite visualizar de manera más precisa los momentos previos, durante y posteriores a la ejecución de las actividades, facilitando la identificación, consideración y evaluación del momento en el cual se activa el control.

En este sentido, se puede considerar la cadena de valor como insumo para la definición de los controles, articular con las actividades del proceso y con las causas del riesgo, permitiendo establecer la siguiente alineación:

*Figura No. 4: Cadena de valor del proceso y las tipologías de controles*




*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública, p.60*

De acuerdo con lo anterior los controles se clasifican en:

- **Preventivos:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Afecta el nivel de Probabilidad de ocurrencia del riesgo. (Probabilidad)

- **Detectivos:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Afecta el nivel de Probabilidad de ocurrencia del riesgo y el impacto de acuerdo con su alcance. (Probabilidad e impacto)

- **Correctivos:** control accionado en la salida del proceso una vez el riesgo se ha materializado, y tienen como finalidad mitigar o reducir el impacto generado. Este tipo de controles actúa sobre las consecuencias del riesgo, contribuyendo a disminuir los efectos negativos para la Entidad después de ocurrida la materialización. Generalmente, los controles correctivos se asocian con mecanismos como pólizas de seguro, copias de seguridad (backups), bases de datos alternas u otros instrumentos que permiten responder y recuperarse frente al riesgo materializado. Estos controles suelen implicar costos asociados y tienen una incidencia directa sobre la magnitud del impacto derivado de la materialización del riesgo. (Impacto)

Así mismo de acuerdo con la forma como se ejecutan los controles pueden ser:

- **Manual:** Ejecutados por personas
- **Automático:** Ejecutados por un sistema o software previamente programado o diseñado.

## 1.11. Valoración de Controles.

De acuerdo con la metodología descrita por la Función pública la Unidad de Gestión General – UGG- acoge los mecanismos de valoración de los controles y la calificación de sus atributos o características de eficiencia, conforme con lo que se describe a continuación:

*Tabla No. 5: Valoración de controles*

| **Características de Eficiencia** | | **Peso** |
|---|---|---|
| **Tipo** | Preventivo | 25% |
| | Detectivo | 15% |
| | Correctivo | 10% |
| **Implementación (en implementación no se contempla controles semiautomáticos)** | Automático | 25% |
| | Manual | 15% |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública*

Los demás atributos informativos o de formalización del control, explicados en el numeral 1.10 Estructura para la Describir un Control, no se aplica valoración, pero deben analizarse para garantizar su el diseño, aspectos listados en la tabla 6.

*Tabla No. 6: Análisis atributos formalización del control*

| **Características de Eficiencia** | | **Descripción** |
|---|---|---|
| **Documentación** | Procedimientos | Basados en la estructura del Modelo de Operación 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, guías, Instructivos, Protocolos específicos. |
| **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: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública*

### 1.12. Aplicación de controles en la matriz de severidad.

En el Formato DP-F-009 Matriz de Administración de Riesgos UGG se encuentra parametrizado el cálculo automático del riesgo residual (probabilidad e impacto), conforme a la valoración de los controles registrada en el numeral 1.12 "Valoración de controles".

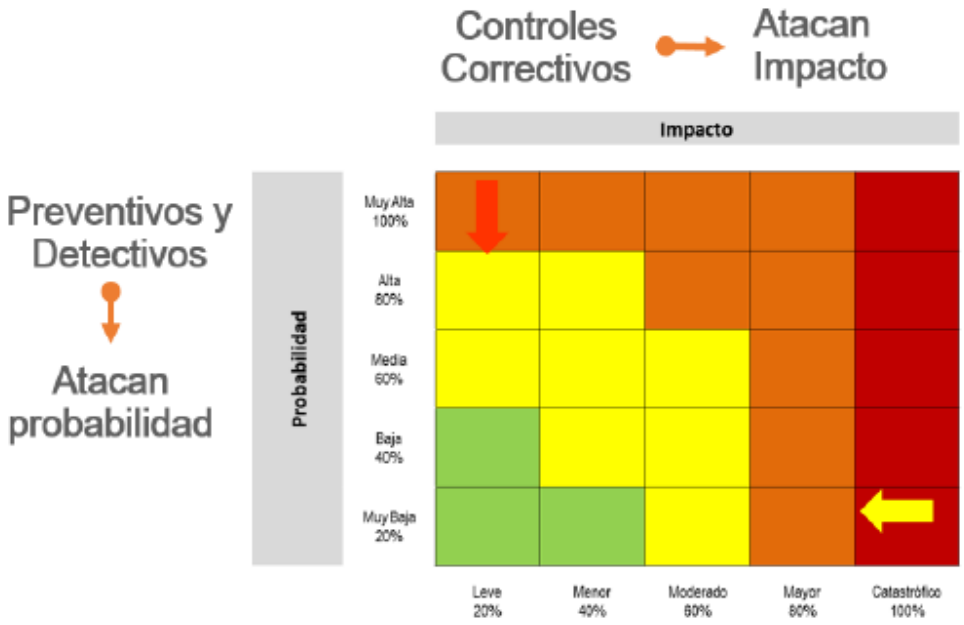
De igual manera, cuando los riesgos y sus respectivos controles son registrados en la plataforma Suite Visión Empresarial (SVE), el sistema realiza de manera automática el cálculo de la nueva probabilidad e impacto del riesgo residual, garantizando la consistencia en la valoración del riesgo.

## PASO 4: VALORACIÓN DE RIESGO RESIDUAL - CALIFICACIÓN DE LOS RIESGOS DESPUÉS DE LA APLICACIÓN DE CONTROLES

Una vez se han evaluado los controles definidos para disminuir probabilidad e impacto de riesgo inherente, la nueva calificación del riesgo recibe el nombre de

riesgo residual después de la aplicación de los controles; de acuerdo con esto se ubica nuevamente en las zonas de severidad en la matriz de calor:

*Figura No. 5: Valoración de Riesgo Residual*




*Fuente: Guía para la gestión integral del riesgo en entidades públicas, versión 7, Función Pública*

## 1.13. Consolidación mapa de riesgos Integral

A partir de la aplicación de cada uno de los pasos metodológicos descritos anteriormente se procede con la elaboración y consolidación del mapa integral de riesgos, establecido por cada proceso y de acuerdo con el diligenciamiento del Formato vigente DP-F-009 "FORMATO MATRIZ ADMINISTRACIÓN DE RIESGOS UGG".

## PASO 5: TRATAMIENTO DE RIESGO RESIDUAL.

### 1.14. Tratamiento de Riesgos.

Se enfoca en el tratamiento que se debe dar al riesgo residual, en caso de identificar falta de controles en procesos, debilidades en los controles o materializaciones de los riesgos.

Cuando se ha determinado el riesgo residual, el siguiente paso es ubicar el resultado para asociar la opción de manejo en la tabla siguiente, mediante la cual el líder del proceso le dará tratamiento:

*Tabla No. 6: Opción de Manejo de Riesgo*

| | Zona de Riesgo | Opción de Manejo |
|---|---|---|
| | Riesgo Bajo | Asumir el riesgo |
| | Riesgo Moderado | Reducir el riesgo |
| | Riesgo Alto | Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir el riesgo |
| | Riesgo Extremo | Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir el riesgo |

*Fuente: Grupo GVP*

Las estrategias de tratamiento sobre el riesgo pueden incluir una o varias de las siguientes opciones:

- **Asumir el riesgo:** Esta opción se aplicará exclusivamente a aquellos riesgos cuyo nivel de riesgo residual se ubique en la zona de riesgo bajo, de conformidad con los criterios definidos en la Tabla No. 6: Opción de Manejo de Riesgo. No obstante, el proceso deberá mantener la implementación de los controles existentes y realizar seguimiento periódico a su comportamiento. En ningún caso, la decisión de asumir el riesgo implicará la eliminación, suspensión o inobservancia de los controles definidos; por el

contrario, el riesgo será asumido garantizando la aplicación permanente y sistemática de los controles previamente establecidos.

- **Reducir el riesgo:** Esta opción se aplicará a aquellos riesgos cuyo nivel de riesgo residual se ubique en la zona de riesgo moderada, de conformidad con los criterios definidos en la Tabla No. 6: Opción de Manejo de Riesgo. Implica la adopción de medidas orientadas a disminuir la probabilidad de ocurrencia del riesgo (acciones de prevención) y/o a mitigar su impacto (acciones de corrección), para lo cual será obligatorio formular e implementar un plan de tratamiento del riesgo. Entre las acciones posibles se encuentran, entre otras, la optimización de procesos, la definición o fortalecimiento de controles, y la mejora de procedimientos operativos.

- **Evitar el riesgo:** Esta opción consiste en adoptar medidas orientadas a eliminar la fuente del riesgo, suprimiendo total o parcialmente el proceso, procedimiento, actividad o condición que da origen a su ocurrencia y, por ende, a su materialización. Para ello, será necesario implementar cambios sustanciales al interior de los procesos, mediante acciones de mejoramiento, rediseño o eliminación de actividades. Evitar el riesgo implica no iniciar o no continuar con las actividades que lo generan, lo cual puede incluir, entre otros, cambios en la infraestructura, ajustes o sustitución de sistemas de información y software, o modificaciones estructurales en la forma de operación del proceso.

- **Compartir o transferir el riesgo:** Esta opción se aplicará a aquellos riesgos cuyo nivel de riesgo residual se ubique en la zona de riesgo alto o extremo, de conformidad con los criterios definidos en la Tabla No. 6: Opción de Manejo de Riesgo. Esta opción consiste en disminuir el efecto del riesgo mediante la distribución o el traspaso parcial de sus posibles consecuencias a otros procesos o partes interesadas, cuando resulte complejo reducirlo internamente a un nivel aceptable o cuando el proceso no cuente con las capacidades técnicas, operativas o especializadas para gestionarlo de manera eficiente, no obstante, es importante precisar que, por regla general, la responsabilidad sobre el riesgo no se transfiere en su totalidad y permanece en cabeza del proceso que identifico el riesgo y le afecta directamente.

  Cuando se opte por compartir o transferir total o parcialmente un riesgo y/o trasladar controles asociados, el líder del proceso deberá

asegurarse de que el tercero seleccionado implemente acciones efectivas de gestión y administración del riesgo, de conformidad con los acuerdos establecidos, y realizar el seguimiento correspondiente para verificar su adecuada ejecución.

## 1.15. Plan de Tratamiento de Riegos.

Los procesos deberán formular e implementar de manera obligatoria un plan de tratamiento para aquellos riesgos cuyo nivel residual se ubique en zonas de riesgo moderada, alta o extrema. Lo anterior, considerando que, si bien la probabilidad de ocurrencia puede disminuir como resultado de la efectividad de los controles, el impacto asociado a una eventual materialización del riesgo continúa siendo significativo para la entidad.

En consecuencia, el plan de tratamiento deberá orientarse al fortalecimiento de los controles existentes, la implementación de acciones adicionales de mitigación y la reducción del nivel de exposición al riesgo, con el fin de salvaguardar el cumplimiento de los objetivos institucionales y prevenir afectaciones relevantes a la operación y a la gestión de la entidad.

El Plan de Tratamiento de Riesgo contiene los siguientes campos: actividades, responsables, fecha de inicio, fecha de finalización y evidencia, para cumplir las acciones correspondientes como se muestra en la figura 6.

*Figura No. 6: Plan de tratamiento*

| OPCIÓN DE MANEJO | TRATAMIENTO | | | | |
|---|---|---|---|---|---|
| | Actividad | Responsable | Fecha de inicio | Fecha de finalización | Evidencia |
| | | | | | |

*Fuente: Grupo GVP*

El plan de tratamiento se cargará a través del módulo de planes en la suite visión, y las actividades serán asignadas al gestor interno de valor público o a quien el líder del proceso designe por cada proceso, quien será responsable de cargar las evidencias de manera semestral, siguiendo lo establecido en cada proceso.

### 1.16. Seguimiento y Monitoreo de riesgos

Se realizará de acuerdo con lo descrito en el numeral 7. Seguimiento, Monitoreo y Revisión de Riesgos descritos en la Guía Gestión Integral de Riesgos en la Unidad de Gestión General.

| | |
|---|---|
| **Elaborado por:** | ***TE. Maira Gimena Botina Benavides*** |
| **Cargo:** | ***Asesora Grupo de Gestión y Valor Público*** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |
| **Revisado por:** | **CT. Monica Soraya Castillo Gonzalez** |
| **Cargo:** | **Coordinadora Grupo de Gestión y Valor Público** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |
| **Aprobado por:** | ***Gloria Stefany Cuesta Andrade*** |
| **Cargo:** | ***Directora de Planeación y Presupuesto*** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |

# *Anexo 4*

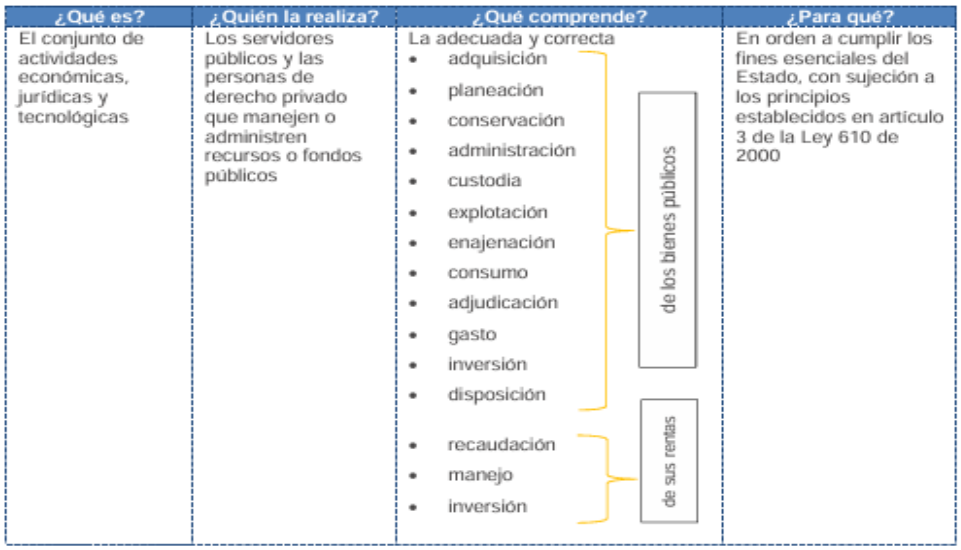
# *"Metodología para la gestión de riesgos Fiscales"*

## 1. Definición y elementos del riesgo fiscal

Son aquellos riesgos que puedan provocar **daño patrimonial al estado** de acuerdo con lo establecido en la "Ley 610 de 2000[1], representado en la disminución, perjuicio, detrimento, perdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del estado", relacionados con la posibilidad de que se generen impactos negativos sobre los recursos públicos, el patrimonio del Estado o la sostenibilidad fiscal de la entidad, como consecuencia de decisiones, actuaciones u omisiones en la gestión presupuestal, financiera, contractual, contable o en el manejo de los recursos públicos.

El riesgo fiscal no es solo la pérdida de dinero; es la incertidumbre sobre la ocurrencia de una conducta que genera un daño real al patrimonio público. De acuerdo con lo anterior es importante tener en cuenta el concepto y los componentes que se explican en la Guía de la Función Pública así:

*Figura No.1. Concepto gestión fiscal - componentes*




*Fuente: Guía para la gestión integral del riesgo en entidades públicas V7 - DAFP*

[1] Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías

## 2. Control Fiscal Interno y Prevención del Riesgo Fiscal

La Unidad de Gestión general del Ministerio de defensa bajo el marco de aplicabilidad de riesgo fiscal en los diferentes procesos obligados a examinar su identificación y tratamiento, sometiendo al control fiscal en un enfoque preventivo que se potencia con el control interno, a partir del cumplimiento de la premisa que el Sistema de control interno es el conjunto de mecanismos y medidas que toma una administración para proveer una seguridad razonable respecto al logro de los resultados, como lo describe la Función Pública en su guía para la gestión integral de riesgos Versión 7.

En este sentido en necesario entender la figura de gestor fiscal dentro de la entidad así:

***"Gestor Fiscal:*** *comprende los jefes de entidad, ordenadores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro entre otros roles cuyas funciones u obligaciones indican en la gestión fiscal."*[2]

Quienes desarrollan el rol de gestor fiscal, serán los llamados en identificar riesgos fiscales en primera instancia para la entidad, siendo estos los procesos de Gestión Administrativa, Gestión Contractual, Gestión Presupuestal, Gestión Financiera, Gestión Logística, TICs Sectorial y Gerentes de Proyectos de Inversión vigentes, aplicando la metodología descrita en el numeral 3. "Metodología para levantamiento de riesgos Fiscales"

## 3. Metodología para levantamiento de riesgos Fiscales

De acuerdo con los lineamientos de la Guía para la Gestión Integral del Riesgo (V.7), la administración del riesgo fiscal se establece como un deber ineludible de cada gestor fiscal quienes son los garantes directos de la protección de los recursos y bienes, asegurando que cada acción de control salvaguarde los intereses patrimoniales del Estado, dentro del alcance del Ministerio de Defensa Nacional-UGG.

La metodología articula los principios de eficiencia y economía con las etapas de la Guía V7 del DAFP. Su enfoque principal es la supervisión de

[2] Concepto tomado de: Guia para la gestión integral de riesgo en Entidades Públicas, Versión 7, p. 72

los procesos de gestión fiscal, orientada a la prevención de daños patrimoniales bajo el marco normativo de la Ley 610 de 2000 y el Decreto 403 de 2020.

Así mismo, se desarrolla el paso a paso para realizar la identificación, clasificación, valoración y control del riesgo fiscal, sin que estos no tengan un enfoque integral dentro de la definición de los demás tipos de riesgos administrados en la entidad, sino que se detallan con la especificidad correspondiente.

*Tabla No. 1. Metodología Riesgos Fiscales*

| **Pasos** | **Acción clave (enfoque riesgo fiscal)** |
|---|---|
| **Contexto** | Identificar los procesos críticos con incidencia fiscal, como compras estratégicas, contratación y manejo de inventarios de bienes públicos. |
| **Identificación** | Detectar eventos de riesgo fiscal asociados a posibles acciones u omisiones (Negligencia, fallas de supervisión, debilidades de control) que puedan generar detrimento patrimonial. |
| **Valoración** | Estimar la probabilidad de ocurrencia y el impacto del efecto dañoso sobre los recursos públicos y la operación institucional. |
| **Controles** | Diseñar o fortalecer controles preventivos, detectivos y correctivos orientados a mitigar la causa raíz del riesgo fiscal. |
| **Tratamiento** | Definir e implementar acciones para reducir la probabilidad o el impacto del riesgo fiscal identificado. |
| **Monitoreo** | Realizar seguimiento continuo al comportamiento del riesgo y a la efectividad de los controles, mediante instancias de control interno. |

*Fuente: Elaboración propia basado en la Guía Integral de Riesgos V7 - DAFP*

## Paso 1. Definición del contexto

Se analizan los factores internos y externos que inciden en la gestión fiscal:

- Contexto externo: Normativa aplicable (incluyendo regímenes especiales de contratación), condiciones del mercado, proveedores estratégicos y compromisos institucionales.

- Contexto interno: Identificación de procesos, responsables de la gestión fiscal (ordenadores del gasto, supervisores, interventores) y puntos críticos donde se administran recursos o bienes públicos.

## Paso 2. Identificación de Riesgos Fiscales

Para la identificación del riesgo fiscal es necesario tener en cuenta los siguientes pasos:

*Figura No.2. Pasos para la identificación del riesgo fiscal*


*Fuente: Guía para la gestión integral del riesgo en entidades públicas V7 – DAFP*

### 2.1. Identificar puntos de riesgo fiscal y las circunstancias Inmediatas.

***Los puntos de riesgo fiscal*** *son eventos en los que potencialmente se genera riesgo fiscal, es decir, son las actividades propias de la gestión fiscal, en cuanto a las* ***circunstancias inmediatas*** *son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo, DAFP (2025).*

Para la identificación de estos componentes se plantea que, en sesiones con el líder del proceso, Coordinadores, asesores de nivel directivo y demás servidores pertenecientes al proceso, apliquen las siguientes preguntas orientadoras:

*Tabla No.2. Preguntas orientadoras para identificar puntos de riesgo fiscal y circunstancias inmediatas*

| **Preguntas y criterios para la identificación** | **Sirve para identificar** |
|---|---|
| ¿En qué Actividades y/o funciones que desarrolla el proceso se realiza gestión fiscal? | Puntos de riesgo fiscal |
| ¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal | Puntos de riesgo fiscal y |

| | |
|---|---|
| y Circunstancias Inmediatas", son aplicables a la entidad? (numeral 2.1.1) | circunstancias inmediatas |
| Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-.<br>**Nota 1:** Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.<br>**Nota 2:** Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.<br>**Nota 3:** Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado.<br>**Nota 4:** La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces. | Puntos de riesgo fiscal y circunstancias inmediatas |
| En un ejercicio autocrítico, realista y objetivo, ¿cuáles son las causas de los hallazgos fiscales identificados por el ente de | Circunstancias inmediatas |

| | |
|---|---|
| control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años?<br><br>**Nota:** Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control. | |

*Fuente: Adopción de Guía para la gestión integral del riesgo en entidades públicas V7 – DAFP*

### 2.1.1. CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Tomado del Anexo 3 CAPÍTULO: Identificación y valoración de Riesgos Fiscales y Diseño de Controles para su Prevención y Mitigación, de la Función Pública:

_____

*Introducción*

*Como resultado de la metodología de investigación que ha venido implementando el Semillero de Investigación de la Academia de la Gestión Pública desde el año 2018, fue posible identificar los principales puntos de riesgo fiscal y circunstancias inmediatas de dichos riesgos, mediante el estudio de: i) los avances que los diferentes órganos de control tienen frente a la definición de riesgo fiscal y la identificación de los principales riesgos fiscales en sus sujetos vigilados, ii) el estudio de fallos con responsabilidad fiscal en firme, emitidos tanto por contralorías territoriales como por la Contraloría General de la República.*

*Así las cosas, los puntos de riesgo fiscal que se enuncian en este catálogo indicativo y enunciativo corresponden a actividades que representan 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 y que potencialmente pueden generar un efecto dañoso al patrimonio público.*

*Este listado enunciativo y no restrictivo, también posibilita identificar y conocer las Circunstancias Inmediatas más comunes en la gestión pública, que se derivan de los Puntos de Riesgo Fiscal.*

*Así las cosas, como resultado del análisis de más de 130 fallos con responsabilidad fiscal tanto de contralorías territoriales como de la Contraloría General de la República, fue posible identificar 50 puntos de riesgo fiscal e igual número de circunstancias inmediatas, así:*

| **Id Referencia** | **Puntos de Riesgo Fiscal** ***Actividad en la que potencialmente se origina el riesgo fiscal*** | **Circunstancia Inmediata** ***Situación por la que se presenta el riesgo*** |
|---|---|---|
| **1** | Cumplimiento de las normas y obligaciones ante autoridades | Pago de multas, cláusulas penales o cualquier tipo de sanción |
| **2** | Cumplimiento de obligaciones | Pago de Intereses moratorios |
| **3** | Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad. | Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente |
| **4** | Liquidación de impuestos | Mayor valor pagado por concepto de impuestos |
| **5** | Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad | Saldos o recursos a favor no cobrados |
| **6** | Custodiar de los bienes muebles de la entidad | Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad |
| **7** | Avalúos a bienes inmuebles de la entidad | Error en los avalúos, afectando el valor de venta y/o negociación de un bien público |

| Id Referencia | Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal* | Circunstancia Inmediata *Situación por la que se presenta el riesgo* |
|---|---|---|
| **8** | Custodiar de los bienes muebles de la entidad | Daño en bienes muebles de propiedad de la entidad |
| **9** | Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad | Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado |
| **10** | Pago de sentencias y conciliaciones | Intereses moratorios por pago tardío de sentencias y conciliaciones |
| **11** | Instrucción del Comité de Conciliación para iniciar acción de repetición | Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado |
| **12** | Informe que acredite o anuncie la existencia de perjuicios generados a la entidad | Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios |
| **13** | Contratación de bienes o servicios | Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad |
| **14** | Contratación de bienes | Compra o inversión en bienes innecesarios o suntuosos |
| **15** | Contratación de estudios y diseños | Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad |

| Id Referencia | Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal* | Circunstancia Inmediata *Situación por la que se presenta el riesgo* |
|---|---|---|
| **16** | Suscripción de contratos de estudios y diseños | Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia |
| **17** | Suscripción de contratos | Sobrecostos en precios contractuales |
| **18** | Suscripción de contratos | Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron |
| **19** | Suscripción de contratos | No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad |
| **20** | Suscripción de contratos | No exigir garantía única de cumplimiento contractual |
| **21** | Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento | Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley |
| **22** | Pagos efectuados a contratistas | Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad. |
| **23** | Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor | Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio |

| Id Referencia | Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal* | Circunstancia Inmediata *Situación por la que se presenta el riesgo* |
|---|---|---|
| **24** | Modificaciones contractuales firmadas | Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante |
| **25** | Giros efectuados por concepto de anticipo contractual | Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo |
| **26** | Giros efectuados por concepto de anticipo contractual | Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público |
| **27** | Reconocimiento y pago de desequilibrio contractual | Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad |
| **28** | Firma de actas contractuales de recibo parcial o final | Errores o imprecisiones en las actas de recibo parcial o final |
| **29** | Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales) | Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto |
| **30** | Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones) | Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato |
| **31** | Actos administrativos sancionatorios contractuales emitidos y ejecutoriados | Cuantificación errada de multa o clausula penal |
| **32** | Obras recibidas a satisfacción | Colapso o fallas en la estabilidad de la obra |

| Id Referencia | Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal* | Circunstancia Inmediata *Situación por la que se presenta el riesgo* |
|---|---|---|
| **33** | Pagos finales efectuados a contratistas | Ejecución de un alcance inferior al contratado y pago total del contrato |
| **34** | Actas de recibo final a satisfacción firmadas | Infuncionalidad de lo ejecutado |
| **35** | Contratos finalizados | Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio |
| **36** | Pagos efectuados a contratistas | Inadecuada deducción de impuestos, tasas o contribuciones al contratista |
| **37** | Pagos por concepto de comisión a éxito | Pago de comisiones a éxito sin debida justificación |
| **38** | Actas de liquidación suscritas | Suscripción de acta de liquidación con imprecisiones de fondo |
| **39** | Actas de liquidación suscritas | Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista |
| **40** | Contratos finalizados en los que se contemplaba o requería liquidación. | Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad |
| **41** | Actas de liquidación suscritas | Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades |
| **42** | Bienes u obras recibidas a satisfacción | Deterioro del bien u obra por indebido mantenimiento |

| Id Referencia | Puntos de Riesgo Fiscal *Actividad en la que potencialmente se origina el riesgo fiscal* | Circunstancia Inmediata *Situación por la que se presenta el riesgo* |
|---|---|---|
| **43** | Actas de recibo final a satisfacción firmadas | Suscripción de acta de recibo final con imprecisiones de fondo |
| **43** | Reintegro de saldos a favor de la entidad o pagos por parte de deudores | Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo) |
| **44** | Predios adquiridos | Adquisición de predios sin las especificaciones técnicas requeridas |
| **45** | Pérdida de tenencia de bienes de la entidad | Pérdida de la tenencia de bienes inmuebles de la Entidad |
| **46** | Pago de subsidios, transferencias o beneficios a particulares | Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones |
| **47** | Pago de subsidios, transferencias o beneficios a particulares | Pago de subsidio u otros beneficios a personas fallecidas |
| **48** | Pago de subsidios, transferencias o beneficios a particulares | Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley |
| **49** | Pago de subsidios, transferencias o beneficios a particulares | Pago de subsidios por encima del beneficio otorgado |
| **50** | Deudas a favor de la entidad | Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial |

*Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2022*[3]

## 2.2. Identificar áreas de impacto

En el marco de la gestión fiscal, se han identificado escenarios críticos donde el uso inadecuado de los recursos impacta directamente la capacidad institucional, estos riesgos se agrupan en las siguientes categorías operativas:

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 entidad en caso de materializarse el riesgo. Para definir de manera correcta el área de impacto, al momento de identificar y redactar riesgos fiscales, es fundamental tener claro el concepto de patrimonio público a partir de las tres expresiones que se derivan del artículo 6 de la Ley 610 de 2000:

*Figura No.3. Areas de impacto riesgos Fiscales*


*Fuente: Elaboración propia basado en la Guía Integral de Riesgos V7 - DAFP*

[3] Anexo3 Función Pública: Este catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias Inmediatas, es el resultado del análisis de investigaciones previas y del estudio detallado de información sobre:

*(i)* Fallos con responsabilidad fiscal, en firme, emitidos en los últimos 3 años, por una muestra de 10 de las contralorías territoriales mejor calificadas en 2020, según el criterio de desempeño integral, el cual corresponde a evaluación realizada por la Auditoría General de la República.

*(ii)* Muestra aleatoria de fallos con responsabilidad fiscal, en firme, emitidos por la Contraloría General de la República en los últimos 3 años.

*(iii)* Listado de hallazgos fiscales por temáticas, consolidado por la Auditoría General de la República, 2021.

## 2.3. Identificar el efecto económico

*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. DAFP (2025).*

## 2.4 Identificar la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (Acción u omisión) que provoca la disminución, perjuicio, detrimento o perdida de recursos, bienes y/o intereses públicos. La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal (efecto dañoso), a continuación, se presentan algunos pasos necesarios para su identificación.

*Figura No.4. Relación causa raíz / Efecto Dañoso*


*Fuente: Elaboración propia basado en la Guía Integral de Riesgos V7 – DAFP*

De acuerdo con lo anterior los elementos clave para logar una identificación de riesgo fiscal se deben reflejar en el siguiente resultado:

### Ejemplo identificación de riesgo fiscal

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega

un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago. A continuación, en la tabla se desarrollan los pasos antes explicados:

| Paso | Identificación |
|---|---|
| **Punto de Riesgo:** **(actividad de la gestión fiscal)** | Administración de inmuebles en arrendamiento al servicio de la entidad |
| **Circunstancia inmediata:** **(situación en la que se presenta el riesgo)** | Pago de intereses moratorios en contrato de arrendamiento |
| **Área de Impacto:** **(patrimonio público afectado)** | Recursos públicos de la entidad |
| **Efecto económico:** **(potencial daño al patrimonio)** | Disminución de recursos disponibles equivalente al monto pagado por concepto de intereses moratorios |
| **Causa raíz:** **(potencial acción u omisión)** | Omisión de pago oportuno del canon de arrendamiento |

*Fuente: Guía para la gestión integral del riesgo en entidades públicas V7*

*Tabla 3. Pasos para identificación de la causa raíz*

| Paso | Enfoque metodológico (riesgo fiscal) | Aplicación |
|---|---|---|
| **1. Identificación del efecto dañoso** | Se define el posible daño al patrimonio público, como punto de partida del análisis fiscal. | Detrimento patrimonial por pagos de bienes o servicios que no cumplen con las condiciones contractuales. |
| **2. Definición del riesgo (evento)** | Se describe el evento que puede materializar el daño, en línea con la estructura causa–evento–consecuencia de Función Pública. | Posibilidad de realizar pagos sin verificar el cumplimiento de obligaciones contractuales. |
| **3. Identificación de causas** | Se determinan las situaciones que originan el riesgo, diferenciando factores internos (procesos, controles) y externos. | Debilidades en supervisión contractual, falta de controles y seguimiento insuficiente. |
| **4. Análisis de causa raíz (hecho generador)** | Se profundiza mediante análisis causa–efecto o técnica de los "¿Por qué?" hasta identificar la acción u omisión concreta que genera el riesgo fiscal. | Omisión en la verificación oportuna y documentada del cumplimiento contractual por parte de la supervisión. |
| **5. Relación causa–evento–efecto** | Se valida la trazabilidad entre causa raíz, evento y efecto dañoso, asegurando coherencia técnica. | La omisión en supervisión → permite incumplimientos → genera pagos indebidos → |

| | | |
|---|---|---|
| | | produce detrimento patrimonial. |
| **6. Orientación al control** | Los controles deben diseñarse para atacar directamente la causa raíz, conforme a la gestión del riesgo fiscal. | Fortalecimiento de supervisión, implementación de listas de chequeo, seguimiento documental y evidencias de cumplimiento. |

*Fuente: Elaboración propia basado en la Guía Integral de Riesgos V7 - DAFP*

## 2.3 Descripción del Riesgo Fiscal

De acuerdo con los lineamientos de la Guía para la Gestión Integral del Riesgo (V.7), Para redactar un riesgo fiscal, se debe tener en cuenta:

- Iniciar con la expresión: Posibilidad de, dado que nos estamos refiriendo al evento potencial.
- Impacto: corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre el área de impacto (recursos públicos, bienes o intereses patrimoniales de naturaleza pública).
- Circunstancia inmediata: corresponde al cómo. Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera.
- Causa Raíz: corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño. Es la condición necesaria del riesgo, de tal forma que, si ese hecho no se produce, el daño no se genera.

*Figura No.5. Descripción del riesgo*


*Fuente: Guía para la gestión integral del riesgo en entidades públicas V7*

Continuando con el ejemplo de identificación de riesgo se procede a la redacción del riesgo fiscal, así:

Posibilidad de efecto dañoso sobre los **recursos de la entidad** por la generación de intereses m oratorios en contrato de arrendamiento a **causa de la omisión** en el pago oportuno del canon pactado

**Conclusión:** El hecho generador del daño no es el pago de la deuda ya que esta es una acción diligente que da cumplimiento a una obligación adquirida. La causa raíz corresponde a la omisión de pago oportuno y el riesgo fiscal al potencial daño representado en los intereses moratorios pagados. Ante dicha situación, se requiere la activación de controles correctivos para evitar que se materialice el daño patrimonial (Hallazgo fiscal), tales como 82 el reembolso del monto correspondiente a los intereses moratorios y controles preventivos para que no se vuelva a presentar la omisión (causa raíz).

**Paso 2: Análisis y Valoración del Riesgo**: se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

- Probabilidad: se determina según el número de veces que se pasa por el punto de riesgo.
- Impacto: considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico.
- Matriz de Calor: zona de riesgo inicial (Extremo, Alto, Moderado o Bajo).

**Paso 3: Diseño y Evaluación de Controles**: se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

- Tipos de Control: Pueden ser preventivos, detectivos o correctivos.
- Atributos: Responsable, acción, complemento

**Paso 4: Valoración De Riesgo Residual:** se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

**Paso 5: Tratamiento del Riesgo:** se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

Definir acciones para reducir, compartir o evitar la probabilidad o el impacto del riesgo residual. Esto suele implicar el fortalecimiento de las Supervisiones e Interventorías y la capacitación en Responsabilidad Fiscal (Ley 610/2000).

| | |
|---|---|
| **Elaborado por:** | ***TE. Maira Gimena Botina Benavides*** |
| **Cargo:** | ***Asesora Grupo de Gestión y Valor Público*** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |
| **Revisado por:** | **CT. Monica Soraya Castillo Gonzalez** |
| **Cargo:** | **Coordinadora Grupo de Gestión y Valor Público** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |
| **Aprobado por:** | ***Gloria Stefany Cuesta Andrade*** |
| **Cargo:** | ***Directora de Planeación y Presupuesto*** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |

# *ANEXO 5*

# *"METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION"*

El presente anexo técnico tiene como propósito incorporar, dentro de los lineamientos de la Gestión Integral del Riesgo de la Unidad de Gestión General del Ministerio de Defensa, los aspectos relacionados con la Gestión de Riesgos de Seguridad de la Información, en concordancia con lo establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7, expedida por el Departamento Administrativo de la Función Pública. Lo anterior permitirá implementar de manera estructurada este proceso, con el fin de fortalecer la confianza en el uso del entorno digital y garantizar la protección y aseguramiento de los activos de información de la entidad.

En este sentido, el fortalecimiento de la postura de seguridad de la entidad inicia con la identificación sistemática y rigurosa de los activos de información, permitiendo reconocer aquellos elementos críticos que requieren protección prioritaria. Este ejercicio constituye la base para el desarrollo de un análisis integral de riesgos, amenazas y vulnerabilidades, orientado a evaluar de manera objetiva los potenciales impactos sobre el entorno digital institucional. Con fundamento en lo anterior, se procede a la definición e implementación de controles, diseñados para mitigar los riesgos identificados, y se consolida el proceso mediante mecanismos de reporte y seguimiento que aseguran la trazabilidad, la toma de decisiones informadas y la mejora continua de la seguridad de la información.

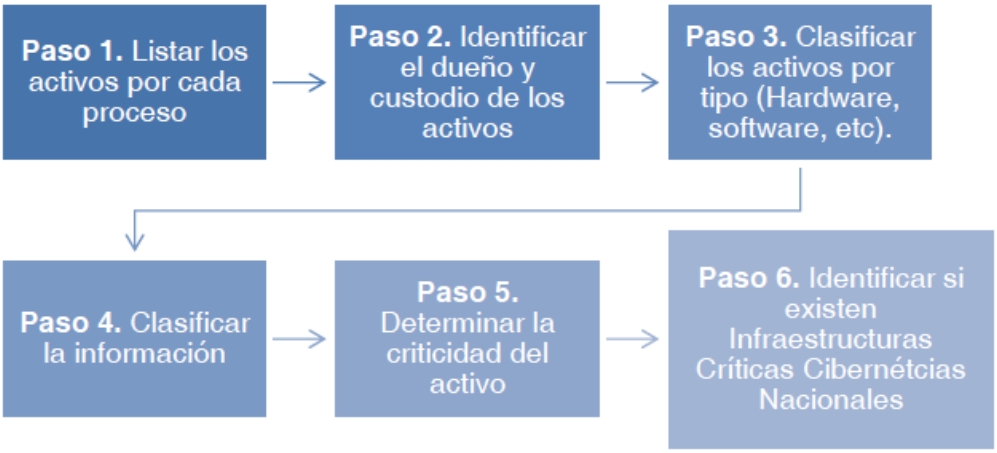
## PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

### *1.1.* Identificación de los riesgos:

En primer lugar, se debe identificar los activos de información de acuerdo con lo establecido en la Ley 594 del 2000, Ley 1712 de 2014, Decreto 103 de 2015, Decreto 1080 de 2015 y Norma ISO 27001, mediante el desarrollo de las actividades descritas en los "Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional" del MSPI.

A continuación, se comparte la ruta para la identificación de activos de información.

*Figura No 1. Ruta para la identificación de activos de información*




*Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.*

La Unidad de Gestión General aplica estos pasos de la siguiente manera:

- Paso 1: Listar los activos por cada proceso: Para cada activo se deben registrar los siguientes datos:
  - Despacho: Unidad o área de proceso a la que pertenece la dirección en la que reside el activo
  - Dirección: Dirección o dependencia adscrita al proceso identificado al que pertenece el activo.
  - Identificador: Número consecutivo que permita la identificación única del activo dentro del inventario
  - Tipo: define el tipo de Activo de Información entre ellos información y datos de la entidad, Sistemas de información y aplicaciones de software, Dispositivos de tecnologías de la información Hardware, Soporte para almacenamiento de información, servicios, recursos humanos, instalaciones, redes,
  - Grupo: dependencia que está identificando el activo de información
  - Serie documental: Serie documental del área, dependencia o proceso que se encuentra identificando el Activo
  - Subserie documental: Subserie documental del área, dependencia o proceso que se encuentra identificando el Activo
  - Nombre: Nombre completo del activo de información
  - Descripción: Descripción resumida de manera clara para identificar el activo de información.
  - Propietario del Activo: Nombre del área, dependencia, proceso responsable de producir el activo de información
  - Fecha de Registro de la información en la matriz: Fecha en la que el activo de información fue incluido en la matriz (inventario de activos).

- Nombre del responsable de la información (custodio del activo): Corresponde al nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección
- Fecha de Ingreso del activo al archivo: Fecha en la que el activo ingresa al archivo de gestión.
- Soporte de registro: de acuerdo con Decreto 2609 de 2012 puede ser Físico – Digital – N/A para el resto de los tipos de activos
- Medio de conservación: De acuerdo con el Decreto 2609 de 2012 Archivo Institucional Es la instancia administrativa de custodiar, organizar y proteger.
- Formato: Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: Hoja de cálculo, imagen, audio, video, documento de texto, etc
- Idioma: Establece el idioma, lengua o dialecto en que se encuentra la información

- **Paso 2**. Identificar el dueño y custodio de los activos: refiere al Nombre del responsable de la información (Custodio del activo) nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección.

- **Paso 3**. Clasificar los activos por tipo (Hardware, software,etc): Corresponde al proceso mediante el cual los activos de información se organizan y agrupan según su naturaleza y función dentro de la entidad, tales como hardware, software, información, servicios, recurso humano e instalaciones. Esta clasificación permite identificar de manera estructurada los componentes que soportan los procesos institucionales, facilitando su gestión, protección, análisis de riesgos y la aplicación de controles de seguridad acordes a cada tipo de activo

- **Paso 4.** Clasificar la información: De acuerdo con Disponibilidad, Integridad y Confidencialidad se definieron tres (3) niveles que permiten determinar el valor general o criticidad del activo en la entidad": Alta, Media y Baja, que corresponden con Criterios de Clasificación para cada una de las propiedades de la Información

*Tabla No. 1 Criterios de Clasificación*

| CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD |
|---|---|---|
| INFORMACIÓN PÚBLICA RESERVADA | ALTA (A) | ALTA (1) |
| INFORMACIÓN PÚBLICA CLASIFICADA | MEDIA (M) | MEDIA (2) |

| CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD |
|---|---|---|
| INFORMACIÓN PÚBLICA | BAJA (B) | BAJA (3) |
| NO CLASIFICADA | NO CLASIFICADA | NO CLASIFICADA |

***Fuente:*** *Tomado de Guia para la Gestión Integral de Riesgos (V7), Función Pública - Ministerio de Tecnologías de la Información y las Comunicaciones, 2025*

El nivel de clasificación del activo corresponderá con el resultado de la sumatoria de la tabla de criterios de clasificación, que se muestra en la tabla No. 1.

*Tabla No. 2. Niveles de Clasificación*

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

***Fuente:*** *Tomado de Guia para la Gestión Integral de Riesgos (V7), Función Pública - Ministerio de Tecnologías de la Información y las Comunicaciones, 2025*

- **Paso 5.** Determinar la criticidad del activo:
  De acuerdo con la Guia para la Gestión Integral de Riesgos (V7), de la Función Pública, el nivel de Criticidad del activo corresponde a:

  - Es Infraestructura Critica cibernética Nacional
  - Información publicada
  - Lugar de consulta o ubicación

El siguiente bloque corresponde con el Índice de información clasificada y reservada

- Objeto legítimo de la excepción
- Fundamento constitucional o legal
- Fundamento jurídico de la excepción
- Excepción total o parcial
- Fecha de clasificación (DD/MM/AAAA)

- Tiempo de clasificación

El siguiente bloque corresponde con los activos de información que contienen datos personales

- ¿Contiene datos personales?
- ¿Contiene datos personales de niños, niñas o adolescentes?
- Tipos de datos personales
- Finalidad de la recolección de los datos personales
- Existe la autorización para el tratamiento de los datos personales

- **Paso 6**. Identificar si existen Infraestructuras Criticas Cibernéticas Nacionales: Se define si el activo corresponde con los criterios de Infraestructura Critica cibernética descritos en los "lineamiento para la identificación de las infraestructuras críticas cibernéticas" del MSPI.

"Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información por los líderes de los procesos, se debe enviar la matriz para su consolidación y validación por parte de la Oficina Asesora Jurídica para finalmente ser presentada ante el Comité Institucional de Gestión y Desempeño."

El resultado de esta actividad es la Matriz del Inventario de Activos de Información que es el insumo principal para la Gestión de Riesgos de Seguridad de la Información proceso que se encuentra descrito en la Guía "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas", de la cual se debe establecer según el nivel de criticidad a cuáles activos se les realizará el correspondiente análisis de riesgos.

Matriz de Riesgos de Seguridad de la Información: Con base en la criticidad se realiza el proceso de gestión de riesgos, la cual registra en la Matriz de Riesgos de Seguridad de la Información, con respecto al activo de información se registran los siguientes datos:

*Tabla No. 3. Matriz de Riesgos de Seguridad de la Información*

| **MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** | | | |
|---|---|---|---|
| **Despacho** | **Referencia** | **Activo de Información** | **Tipo de Activo** |
| | | | |

***Fuente:*** *ajustado a la entidad Tomado como base la Guia para la Gestión Integral de Riesgos (V7), Función Pública - Ministerio de Tecnologías de la Información y las Comunicaciones, 2025*

Para el diligenciamiento de la anterior matriz se describe cada aspecto:

**Despacho:** Proceso al cual se encuentra asignado el activo de información.
**Referencia:** Es el número del ítem del activo de información.
**Activo de Información:** Es el nombre del activo de información.
**Tipo de Activo:** Corresponde a una de las siguientes categorías:

- ✓ Información
- ✓ Software
- ✓ Hardware
- ✓ Servicios
- ✓ Intangibles
- ✓ Infraestructura crítica cibernética nacional
- ✓ Recursos humanos
- ✓ Instalaciones y Otros Servicios

1.2. **Identificación de áreas de factores de riesgo:** Son las fuentes generadoras de riesgos las Amenazas (Causa Inmediata) y las Vulnerabilidades (Causa raíz), de acuerdo con el Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022). Pueden ser Deliberadas (D), fortuitas (F) o ambientales (A)

*Tabla No. 4. Amenazas comunes*

| Tipo | Amenaza | Origen |
|---|---|---|
| **Daño físico** | Fuego | F, D, A |
| | Agua | F, D, A |
| | Contaminación | F, D, A |
| | Accidente Importante | F, D, A |
| | Destrucción del equipo o medios | F, D, A |
| | Polvo, corrosión, congelamiento | F, D, A |
| **Eventos naturales** | Fenómenos climáticos | A |
| | Fenómenos sísmicos | A |
| | Fenómenos volcánicos | A |
| | Fenómenos meteorológicos | A |
| | Inundación | A |

| Tipo | Amenaza | Origen |
|---|---|---|
| **Pérdida de servicios esenciales** | Fallas en suministro de agua o aire acondicionado | A |
| | Pérdida de suministro de energía | A |
| | Falla en equipo de telecomunicaciones | D, F |
| **Perturbación por radiación** | Radiación electromagnética | D, F |
| | Radiación térmica | D, F |
| | Impulsos electromagnéticos | D, F |
| **Compromiso de información** | Interceptación de señales | D |
| | Espionaje remoto | D |
| | Escucha encubierta | D |
| | Hurto de medios o documentos | D |
| | Hurto de equipo | D |
| | Recuperación de medios reciclados o desechados | D |
| | Divulgación | D, F |
| | Datos provenientes de fuentes no confiables | D, F |
| | Manipulación con hardware | D |
| | Manipulación con software | D |
| | Detección de la posición | D, F |
| **Fallas técnicas** | Fallas del equipo | F |
| | Mal funcionamiento del equipo | F |
| | Saturación del sistema de información | F |
| | Mal funcionamiento del software | F |
| | Incumplimiento en el mantenimiento del sistema | F |
| **Acciones no autorizadas** | Uso no autorizado del equipo | D |
| | Copia fraudulenta de software | D |
| | Uso de software falso o copiado | D |
| | Corrupción de los datos | D |
| | Procesamiento ilegal de datos | D |

| Tipo | Amenaza | Origen |
|---|---|---|
| **Compromiso de funciones** | Error en el uso | D, F |
| | Abuso de derechos | D |
| | Falsificación de derechos | D |
| | Negación de acciones | D |
| | Incumplimiento en disponibilidad del personal | D |

*Fuente: Tomado de Guia para la Gestión Integral de Riesgos (V7), Función Pública - Ministerio de Tecnologías de la Información y las Comunicaciones, 2025*

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

*Tabla No. 5. Vulnerabilidades comunes*

| Tipo | Vulnerabilidades |
|---|---|
| **Hardware** | Mantenimiento insuficiente |
| | Ausencia de esquemas de reemplazo periódico |
| | Sensibilidad a la radiación electromagnética |
| | Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) |
| | Almacenamiento sin protección |
| | Falta de cuidado en la disposición final |
| | Copia no controlada |
| **Software** | Ausencia o insuficiencia de pruebas de software |
| | Ausencia de terminación de sesión |
| | Ausencia de registros de auditoría |
| | Asignación errada de los derechos de acceso |
| | Interfaz de usuario compleja |
| | Ausencia de documentación |
| | Fechas incorrectas |
| | Ausencia de mecanismos de identificación y autenticación de usuarios |
| | Contraseñas sin protección |
| | Software nuevo o inmaduro |
| **Red** | Ausencia de pruebas de envío o recepción de mensajes |

| Tipo | Vulnerabilidades |
|---|---|
| | Líneas de comunicación sin protección |
| | Conexión deficiente de cableado |
| | Tráfico sensible sin protección |
| | Punto único de falla |
| **Personal** | Ausencia del personal |
| | Entrenamiento insuficiente |
| | Falta de conciencia en seguridad |
| | Ausencia de políticas de uso aceptable |
| | Trabajo no supervisado de personal externo o de limpieza |
| **Lugar** | Uso inadecuado de los controles de acceso al edificio |
| | Áreas susceptibles a inundación |
| | Red eléctrica inestable |
| | Ausencia de protección en puertas o ventanas |
| **Organización** | Ausencia de procedimiento de registro/retiro de usuarios |
| | Ausencia de proceso para supervisión de derechos de acceso |
| | Ausencia de control de los activos fuera de las instalaciones |
| | Ausencia de acuerdos de nivel de servicio (ANS o SLA) |
| | Ausencia de mecanismos de monitoreo para brechas en la seguridad |
| | Ausencia de procedimientos y/o de políticas en general (uso de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia, etc.) |
| **Hardware** | Mantenimiento insuficiente |
| | Ausencia de esquemas de reemplazo periódico |
| | Sensibilidad a la radiación electromagnética |
| | Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) |
| | Almacenamiento sin protección |
| | Falta de cuidado en la disposición final |
| | Copia no controlada |

| Tipo | Vulnerabilidades |
|---|---|
| **Software** | Ausencia o insuficiencia de pruebas de software |
| | Ausencia de terminación de sesión |
| | Ausencia de registros de auditoría |
| | Asignación errada de los derechos de acceso |
| | Interfaz de usuario compleja |
| | Ausencia de documentación |
| | Fechas incorrectas |
| | Ausencia de mecanismos de identificación y autenticación de usuarios |
| | Contraseñas sin protección |
| | Software nuevo o inmaduro |
| **Red** | Ausencia de pruebas de envío o recepción de mensajes |
| | Líneas de comunicación sin protección |
| | Conexión deficiente de cableado |
| | Tráfico sensible sin protección |
| | Punto único de falla |
| **Personal** | Ausencia del personal |
| | Entrenamiento insuficiente |
| | Falta de conciencia en seguridad |
| | Ausencia de políticas de uso aceptable |
| | Trabajo no supervisado de personal externo o de limpieza |
| **Lugar** | Uso inadecuado de los controles de acceso al edificio |
| | Áreas susceptibles a inundación |
| | Red eléctrica inestable |
| | Ausencia de protección en puertas o ventanas |
| **Organización** | Ausencia de procedimiento de registro/retiro de usuarios |
| | Ausencia de proceso para supervisión de derechos de acceso |
| | Ausencia de control de los activos fuera de las instalaciones |
| | Ausencia de acuerdos de nivel de servicio (ANS o SLA) |

| Tipo | Vulnerabilidades |
|---|---|
| | Ausencia de mecanismos de monitoreo para brechas en la seguridad |
| | Ausencia de procedimientos y/o de políticas en general (uso de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia, etc.) |

***Fuente:*** *Tomado de Guia para la Gestión Integral de Riesgos (V7), Función Pública - Ministerio de Tecnologías de la Información y las Comunicaciones, 2025*

**1.3. Descripción del Riesgo:** Se debe identificar

- ✓ **Tipo de Riesgo:** Este campo solo admite uno de estos 3 valores:
  - Pérdida de Disponibilidad
  - Pérdida de Integridad
  - Pérdida de Confidencialidad

- ✓ **Descripción del Riesgo:** En este campo se describe la situación específica que da como resultado el correspondiente riesgo. De acuerdo con lo descrito en el Anexo 3. "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

- ✓ **Clasificación del Riesgo:** Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad

## PASO 2: ANÁLISIS DE RIESGO INHERENTE - ANTES DE LA APLICACIÓN DE CONTROLES

Se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

- Probabilidad: se determina según el número de veces que se pasa por el punto de riesgo.
- Impacto: considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico.
- Matriz de Calor: zona de riesgo inicial (Extremo, Alto, Moderado o Bajo).

## PASO 3: DISEÑO Y ANÁLISIS DE CONTROLES

3.1. Estructura para la Descripción del Control:
En esta actividad se seleccionan los controles que se establecerán para mitigar los riesgos.

*Tabla No.6 controles*

| No. Control | Control Anexo A | Descripción del Control |
|---|---|---|
| | | |

***Fuente:*** *Tomado de Guia para la Gestión Integral de Riesgos (V7), Función Pública - Ministerio de Tecnologías de la Información y las Comunicaciones, 2025*

**No. Control:** Este campo es un consecutivo de los controles a establecer.
**Control Anexo A:** Este campo corresponde al control seleccionado del Anexo A de la norma 27001:2022. Citar 27001 Anexo A

**Descripción del Control:** Este campo corresponde a una descripción de la forma en la cual el control seleccionado será implementado en la entidad. Validar la descripción del control con base en la estructura establecida en el Anexo 3

## PASO 4: VALORACIÓN DE RIESGO RESIDUAL - CALIFICACIÓN DE LOS RIESGOS DESPUÉS DE LA APLICACIÓN DE CONTROLES

Representa el nivel final de exposición tras la aplicación de los controles evaluados en el paso anterior. Se calcula confrontando el riesgo inherente frente a la efectividad de los controles (Riesgo Inherente - Efecto de los Controles). Este resultado permite a la entidad decidir si el nivel de riesgo es aceptable o si se requieren acciones adicionales dentro de un Plan de Tratamiento de Riesgos para llevarlo a un nivel tolerable. (Ver Anexo 3)

### Consolidación mapa de riesgos Integral

A partir de la aplicación de cada uno de los pasos metodológicos descritos anteriormente se procede con la elaboración y consolidación del mapa de riesgos de seguridad de la información, establecido por cada proceso y de acuerdo con el diligenciamiento del Formato vigente "Matriz de Riesgos de Seguridad de la Información".

## PASO 5: TRATAMIENTO DE RIESGO RESIDUAL.

### 1.4. Tratamiento de Riesgos.

Se enfoca en el tratamiento que se debe dar al riesgo residual, en caso de identificar falta de controles en procesos, debilidades en los controles o materializaciones de los riesgos.

Cuando se ha determinado el riesgo residual, el siguiente paso es ubicar el resultado para asociar la opción de manejo en la tabla siguiente, mediante la cual el líder del proceso le dará tratamiento:

*Tabla No. 7. Opción de Manejo de Riesgo*

| | Zona de Riesgo | Opción de Manejo |
|---|---|---|
| | Riesgo Bajo | Asumir el riesgo |
| | Riesgo Moderado | Reducir el riesgo |
| | Riesgo Alto | Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir el riesgo |
| | Riesgo Extremo | Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir el riesgo |

*Fuente: Guia para la Gestión Integral de Riesgos UGG*

Las estrategias de tratamiento sobre el riesgo pueden incluir una o varias de las siguientes opciones:

- **Asumir el riesgo:** Esta opción se aplicará exclusivamente a aquellos riesgos cuyo nivel de riesgo residual se ubique en la zona de riesgo bajo, de conformidad con los criterios definidos en la Tabla No. 6: Opción de Manejo de Riesgo. No obstante, el proceso deberá mantener la implementación de los controles existentes y realizar seguimiento periódico a su comportamiento. En ningún caso, la decisión de asumir el riesgo implicará la eliminación, suspensión o inobservancia de los controles definidos; por el contrario, el riesgo será asumido garantizando la aplicación permanente y sistemática de los controles previamente establecidos.

- **Reducir el riesgo:** Esta opción se aplicará a aquellos riesgos cuyo nivel de riesgo residual se ubique en la zona de riesgo moderada, de conformidad con los criterios definidos en la Tabla No. 6: Opción de Manejo de Riesgo. Implica la adopción de medidas orientadas a disminuir la probabilidad de ocurrencia del riesgo (acciones de

prevención) y/o a mitigar su impacto (acciones de corrección), para lo cual será obligatorio formular e implementar un plan de tratamiento del riesgo. Entre las acciones posibles se encuentran, entre otras, la optimización de procesos, la definición o fortalecimiento de controles, y la mejora de procedimientos operativos.

- **Evitar el riesgo:** Esta opción consiste en adoptar medidas orientadas a eliminar la fuente del riesgo, suprimiendo total o parcialmente el proceso, procedimiento, actividad o condición que da origen a su ocurrencia y, por ende, a su materialización. Para ello, será necesario implementar cambios sustanciales al interior de los procesos, mediante acciones de mejoramiento, rediseño o eliminación de actividades. Evitar el riesgo implica no iniciar o no continuar con las actividades que lo generan, lo cual puede incluir, entre otros, cambios en la infraestructura, ajustes o sustitución de sistemas de información y software, o modificaciones estructurales en la forma de operación del proceso.

- **Compartir o transferir el riesgo:** Esta opción se aplicará a aquellos riesgos cuyo nivel de riesgo residual se ubique en la zona de riesgo alto o extremo, de conformidad con los criterios definidos en la Tabla No. 6: Opción de Manejo de Riesgo. Esta opción consiste en disminuir el efecto del riesgo mediante la distribución o el traspaso parcial de sus posibles consecuencias a otros procesos o partes interesadas, cuando resulte complejo reducirlo internamente a un nivel aceptable o cuando el proceso no cuente con las capacidades técnicas, operativas o especializadas para gestionarlo de manera eficiente, no obstante, es importante precisar que, por regla general, la responsabilidad sobre el riesgo no se transfiere en su totalidad y permanece en cabeza del proceso que identifico el riesgo y le afecta directamente.

  Cuando se opte por compartir o transferir total o parcialmente un riesgo y/o trasladar controles asociados, el líder del proceso deberá asegurarse de que el tercero seleccionado implemente acciones efectivas de gestión y administración del riesgo, de conformidad con los acuerdos establecidos, y realizar el seguimiento correspondiente para verificar su adecuada ejecución.

## 1.5. Plan de Tratamiento de Riegos.

Los riesgos clasificados como moderados, altos o extremos en la Matriz de Riesgos de Seguridad de la Información deberán contar con un Plan de Tratamiento de Riesgos que detalle las acciones específicas, responsables, recursos, plazos de ejecución y controles implementados para modificar o reducir el nivel del riesgo identificado.

La información consolidada en la matriz permitirá evidenciar el avance del tratamiento, así como las decisiones de aceptación, compartir o mitigaciones adoptadas por los responsables y avaladas por la Alta Dirección, garantizando la trazabilidad y seguimiento dentro del marco del Sistema de Gestión de Seguridad de la Información (SGSI).

| TRATAMIENTO DEL RIESGO | | | | | |
|---|---|---|---|---|---|
| Opción de Tratamiento | Plan de Acción | Control Anexo A | Responsable de Implementar el Tratamiento | Fecha de Inicio del Tratamiento | Fecha de Finalización del Tratamiento |

### Monitoreo del riesgo

El monitoreo del riesgo corresponde a un proceso continuo y sistemático orientado a mantener actualizada la visión del panorama de riesgos de seguridad de la información del Ministerio de Defensa Nacional, considerando la evolución del contexto organizacional, tecnológico, normativo y del entorno de amenazas.

El monitoreo del riesgo considera principalmente:

- Cambios en los activos de información (incorporación, modificación o retiro).
- Aparición de nuevas amenazas, vulnerabilidades o incidentes de seguridad.
- Variaciones en los procesos, tecnologías, estructura organizacional o estrategias institucionales.

El Ministerio de Defensa Nacional (MDN) realizará el monitoreo formal de los riesgos de seguridad de la información con una periodicidad cuatrimestral, a través de los líderes de proceso y sus equipos de trabajo, quienes deberán efectuar el análisis del comportamiento de los riesgos y remitir su respectivo reporte al Oficial de Seguridad de la Información, conforme al siguiente esquema:

- Primer monitoreo: con corte al 30 de abril de cada año.
- Segundo monitoreo: con corte al 31 de agosto.
- Tercer monitoreo: con corte al 31 de diciembre.

Cada reporte de monitoreo deberá ser enviado a más tardar dentro de los diez (10) días calendario posteriores a cada fecha de corte establecida.

**Seguimiento del riesgo**

El seguimiento consiste en la verificación periódica del avance, cumplimiento y efectividad de las acciones establecidas en el plan de tratamiento del riesgo.

El seguimiento se activa únicamente después de que el plan de tratamiento ha sido formulado permitiendo:

- Confirmar la ejecución progresiva de las acciones.
- Validar la suficiencia de las evidencias aportadas por los responsables.
- Identificar desviaciones, retrasos o mejoras necesarias.
- Evaluar la reducción real del riesgo residual.
- Determinar la necesidad de revisar o ajustar el plan de tratamiento.

**Revaloración Posterior al Tratamiento**

Una vez implementadas la totalidad de las acciones del plan de tratamiento, el MDN deberá realizar una nueva iteración de valoración del riesgo, con el fin de verificar la eficacia de los controles incorporados y actualizar formalmente el nivel de riesgo residual.

En esta iteración, los controles que hayan sido implementados como parte del tratamiento podrán incorporarse en la "Descripción de los Controles" del riesgo, siempre que cumplan las siguientes condiciones:

- Están implementados en su totalidad.
- Son permanentes y forman parte del control institucional.
- Se cuenta con evidencia verificable de su funcionamiento.

Esta iteración evita alterar la valoración original del riesgo y permite reflejar de forma trazada, objetiva y auditable la reducción lograda mediante el tratamiento, asegurando que la actualización del riesgo residual sea coherente, reproducible y alineada con la metodología institucional.

**Frecuencia del Seguimiento**

La cantidad de seguimientos requeridos depende del tiempo definido para la ejecución del plan de tratamiento, garantizando una verificación proporcional a su duración:

- **Planes de tratamiento con duración igual o mayor a doce (12) meses**
  - Requieren tres (3) seguimientos documentados.
- **Planes de tratamiento con duración entre seis (6) y once (11) meses**
  - Requieren dos (2) seguimientos.
- **Planes de tratamiento con duración igual o menor a seis (6) meses**
  - Requieren un (1) seguimiento.

Cada seguimiento debe registrar:

- Fecha de seguimiento
- Evidencias y medios de verificación
- Responsable del seguimiento y estado

| | |
|---|---|
| **Elaborado por:** | **John Yeferson Valbuena Camacho** |
| **Cargo:** | **Analista en Incidentes de Seguridad informática** |
| **Firma:** | ***Original debidamente firmado reposa en el archivo digital de la Dirección de Tecnologías de la Información y las Comunicaciones*** |
| **Revisado por:** | ***Martha Lucia Sanchez Niño*** |
| **Cargo:** | ***Coordinadora Grupo de Seguridad Digital*** |
| **Firma:** | ***Original debidamente firmado reposa en el archivo digital de la Dirección de Tecnologías de la Información y las Comunicaciones*** |
| **Aprobado por:** | **CR. Adriana Maria Alvarez Moreno** |
| **Cargo:** | **Directora de Tecnologías de la Información y las Comunicaciones (E)** |
| **Firma:** | ***Original debidamente firmado reposa en el archivo digital de la Dirección de Tecnologías de la Información y las Comunicaciones*** |

# *ANEXO 6*

# *"SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA"*

De acuerdo con lo descrito en la Guía para la Gestión Integral del Riesgo en Entidades Públicas (V7) describe que, en cumplimiento de la *Ley 2195 de 2022, que hace obligatorio para las entidades públicas la "prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas que defina el Gobierno nacional" (artículo 31), la Secretaría de Transparencia de la Presidencia de la República sugiere a las entidades obligadas a implementar un Programa de Transparencia y Ética Pública contar con un sistema de gestión que le permita prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de las instituciones del Estado (riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción), de manera integral.*

En este marco, la Unidad de Gestión General (UGG), en cumplimiento de las disposiciones establecidas en la Ley 2195 de 2022 y en el Programa de Transparencia y Ética Pública en adelante PTEP, adoptado por la entidad, define, adopta e implementa el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), conforme a los lineamientos impartidos por el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, como el instrumento institucional para la prevención, identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos de integridad pública que puedan comprometer la legalidad, la transparencia, la honra y el buen nombre de la Unidad de Gestión General.
De acuerdo con lo anterior se proporciona el concepto de integridad pública, así:

1. **INTEGRIDAD PÚBLICA:**

Refiere a la aplicación de los principios y atributos de la gestión institucional que se refiere al ejercicio íntegro, ético, moral, transparente y legal realizado en el ejercicio de las funciones o del servicio que prestan los servidores públicos de Unidad de Gestión General, orientado al cumplimiento de los fines institucionales y del Estado, mediante actuaciones fundamentadas en el código de integridad , los valores, normas y controles que previenen, detectan y corrigen conductas o

eventos que puedan afectar la legalidad, la honestidad, la transparencia y la confianza ciudadana.

Por su parte, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) plantea la adopción de un enfoque de gestión de riesgos orientado a la integridad, el cual reconoce cinco amenazas críticas a la integridad pública. Dichas amenazas se consideran riesgos de integridad pública y, en concordancia con lo establecido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, deben ser identificadas, analizadas, valoradas, tratadas y monitoreadas por las entidades, en el marco del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), como parte integral de la prevención y control de conductas que puedan afectar el ejercicio íntegro del servicio público y la confianza ciudadana.
En este sentido, los riesgos que serán objeto de gestión por parte de la Unidad de Gestión General son los siguientes:

a. **Soborno:**
   Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directa o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona. (Norma ISO 37001:2016).

b. **Fraude:**
   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. (*DAFP (2025).*

c. **Inadecuada gestión del conflicto de intereses:**
   Se presenta cuando los intereses particulares, personales, familiares, económicos o de cualquier otra índole de un servidor público, contratista o tercero vinculado a la gestión institucional, pueden influir, o dar la apariencia de influir, de manera indebida en el ejercicio objetivo, imparcial y transparente de sus funciones, comprometiendo el cumplimiento del interés general y los fines de la Entidad.

*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*. (*DAFP (2025).*

**d. Corrupción:**

*Es todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral (Decreto 1081 de 2015)*

**e. Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP:**

*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. (DAFP 2025)*

**Lavado de Activos:** son acciones u operaciones orientadas a ocultar, encubrir o dar apariencia de legalidad a recursos provenientes de actividades ilícitas, con el fin de incorporarlos al sistema económico o financiero, o de utilizarlos dentro de la operación de una entidad, afectando la legalidad, transparencia y correcto uso de los recursos públicos. Puede presentarse a través de terceros, contratistas, proveedores, donaciones,

convenios, pagos, inversiones, uso de activos o cualquier interacción financiera o administrativa de la entidad.

**Financiación del Terrorismo:** consiste en la provisión, recolección, administración, custodia o uso de fondos, bienes o recursos, de origen lícito o ilícito, con el propósito de apoyar, facilitar o ejecutar actividades terroristas, organizaciones terroristas o a sus miembros, afectando la legalidad, la seguridad nacional, la confianza ciudadana y el cumplimiento de los fines esenciales del Estado y de la entidad.

De acuerdo con la Unidad de Información y Análisis Financiero (UIAF) La Financiación del Terrorismo está relacionada con los fondos, bienes o recursos a los que acceden las organizaciones terroristas o los terroristas para poder costear sus actividades.

**Financiación de la Proliferación de Armas de Destrucción Masiva:** es todo acto que provea fondos o utilice servicios financieros, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, trasiego de material, fraccionamiento, transporte, trasferencia, deposito o uso dual para propósitos ilegítimos en contravención de las leyes nacionales u obligaciones internacionales, cuando esto último sea aplicable[1].

## 2. SISTEMA DE GESTIÓN DE RIESGO DE INTEGRIDAD PÚBLICA

La Unidad de Gestión General (UGG) incorpora e implementa el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), en cumplimiento de lo dispuesto en el Programa de Transparencia y Ética Pública del Ministerio, específicamente en la Línea Estratégica 2.1: Administración de Riesgos.

El SIGRP, a través de la Política Integral de Riesgos, permite la articulación de los diferentes sistemas de gestión de la entidad para la identificación, análisis y tratamiento de los riesgos. En este marco, es posible identificar elementos comunes asociados a la integridad pública, teniendo en cuenta que un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causas factores como el soborno, el fraude, los conflictos de intereses o la corrupción, los cuales pueden facilitar el lavado de activos, la financiación del terrorismo

[1] Tomado de Unidad de Información y Análisis Financiero (UIAF): https://www.uiaf.gov.co/sistema-nacional-ala-cft/lavado-de-activos-y-financiacion-del-terrorismo

o la financiación de la proliferación de armas de destrucción masiva. Por tal razón, la Unidad de Gestión General abordará los riesgos de la integridad pública de manera integral y en estrecha articulación con la gestión del riesgo institucional.

## 2.1 Contexto de la Organización

El ejercicio de Contexto de la Unidad de Gestión General del Ministerio de Defensa se encuentra descrito bajo la Guía Contexto Interno y Externo, DP-G-009, enfocando la metodología en la identificación de Factores Internos (Fortalezas/Debilidades) y Factores Externos (Amenazas/Oportunidades), bajo este marco y en coherencia con lo requerido por el SIGRP, cada proceso deberá también complementar este ejercicio con los siguientes análisis adicionales:

- Análisis de la planta (Servidores Públicos) y estructura de la entidad (Organigrama), así como la identificación de la delegación de la autoridad y el poder decisorio dentro del proceso y de la entidad (Alta Dirección, directivos, jefes de oficina, coordinadores y gerentes de proyecto). Para este ejercicio se podrá tomar como insumo el mapa de redes internas de la entidad, suministrado por el líder de la Línea Estratégica de Redes y Articulación del PTEP.

- Análisis de los grupos de valor o partes interesadas, incluidos los clientes internos y externos, así como aquellas contrapartes con las cuales se presentan interacciones que involucren la prestación o entrega de productos, servicios o el intercambio de recursos.

- Identificación de las zonas geográficas en las que opera el proceso o la dependencia, de acuerdo con la misión institucional y el cumplimiento de las funciones asignadas.

- Análisis de la naturaleza, escala y complejidad del proceso, de la prestación del servicio, del trámite u de otras operaciones administrativas desarrolladas por la dependencia, dirección o proceso, en cumplimiento de los objetivos estratégicos y la misión institucional.

- Identificación de la información relacionada con los contratos y los principales proveedores requeridos para el cumplimiento del objetivo del proceso y de las funciones de la dependencia.

- Análisis de las entidades sobre las cuales la organización ejerce control, así como de aquellas que ejercen control sobre la entidad.

Para este ejercicio se podrá utilizar como insumo el mapa de redes externas de la entidad, proporcionado por el líder de la Línea Estratégica de Redes y Articulación del PTEP.

- Análisis de las interacciones con entidades de otras ramas del poder público, órganos de control u organismos independientes, así como de las interacciones con particulares con los cuales no se tenga un vínculo contractual o formal, tales como actividades de cabildeo. Para este ejercicio se podrá tomar como insumo el mapa de redes externas de la entidad, suministrado por el líder de la Línea Estratégica de Redes y Articulación del PTEP.

## 2.2 Liderazgo del Sistema

De acuerdo con lo establecido en el numeral *2. GOBERNANZA DE LA GESTIÓN DEL RIESGO (ESQUEMA DE LÍNEAS DE DEFENSA)* de la presente guía, donde se establecen roles y responsabilidades de las líneas de defensa y de áreas específicas de la Unidad de Gestión General para el cumplimiento de la gestión integral de riesgos en la entidad, para efectos del SIGRIP, existen unos roles y responsabilidades que deben agregarse a esos niveles de responsabilidad. A continuación, se relacionan en función del esquema de líneas y los roles que existen en los Programas de Transparencia y Ética Pública, así:

*Tabla No. 1. Roles y responsabilidades SIGRIP*

| Línea Estratégica | 3ra Línea | 2da Línea | 1ra Línea |
|---|---|---|---|
| Supervisor del Programa | Auditor del Programa | Administrador del Programa | Ejecutores del Programa |
| • Alta Dirección<br>• Comité Institucional de Gestión y Desempeño.<br>• Subcomité de Coordinación del Sistema de Control Interno. | Oficina de Control Interno, Auditoría Interno o quien haga sus veces. | Dependencia o persona designada por la Alta Dirección | Directivos, líderes de proceso, servidores y colaboradores |
| Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos | Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – | En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP | Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de |

| | | | |
|---|---|---|---|
| para la Integridad Pública – SIGRIP. | SIGRIP, con el propósito de asesorar y recomendar mejoras. | asume la función de cumplimiento. | Gestión de Riesgos para la Integridad Pública – SIGRIP. |

*Fuente: Adaptado de Guía para la gestión integral del riesgo en entidades públicas V7 - Secretaría de Transparencia de la Presidencia de la República, 2025*

De acuerdo con la tabla y lo requerido por la Secretaría de Transparencia de la Presidencia de la República, la segunda línea asumirá el rol de Administrador del programa y **función de cumplimiento** que implica, entre otros aspectos lo siguiente:

- Velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto, y cada uno de sus elementos, promoviendo el cumplimiento de sus disposiciones y apoyando a los líderes de procesos y gestores de riesgo, en la gestión de los riesgos identificados. Para estos efectos, se podrán generar políticas o procedimientos internos, vinculantes para la organización.
- Evaluar el SIGRIP y presentar, en la periodicidad que se establezca, los resultados de la evaluación a la Alta Dirección. Las evaluaciones deberán contemplar, además:
    - Los resultados de la gestión desarrollada en el marco de la función de cumplimiento
    - Los reportes de operaciones generados en el marco de la gestión del riesgo
    - Los planes de mejoramiento del SIGRIP implementados, en el marco del proceso de mejora continua
- Revisar y recomendar la implementación de los lineamientos que el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República, la Unidad de Información y Análisis Financiero, y las entidades de control, expidan en temas relacionados con la gestión del riesgo.
- Promover la adopción de correctivos del SIGRIP y adoptar aquellos que estén dentro de su competencia.
- Articular con las dependencias correspondientes las gestiones pertinentes para la operatividad del SIGRIP, así como el desarrollo de programas internos de capacitación en materia de cumplimiento y gestión del riesgo.
- Proponer a la Alta Dirección la actualización de los elementos del SIGRIP y velar por su comunicación oportuna a todas las partes interesadas.

- Colaborar con el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos que requiera el SIGRIP y aplicarlos según corresponda.
- Establecer los lineamientos institucionales para la aplicación proporcional basada en riesgos de los mecanismos de debida diligencia en el conocimiento de las contrapartes.
- Elaborar y someter a aprobación de la Alta Dirección, los criterios objetivos para la determinación de las operaciones inusuales y sospechosas.
- Reportar a la Unidad de Información y Análisis Financiero, a la Fiscalía General de la Nación o a la autoridad que corresponda, las operaciones intentadas o sospechosas que se hayan identificado conforme a los criterios definidos y el procedimiento institucional adoptado

## 2.3 Política del SIGRIP.

De acuerdo con lo establecido en el numeral *4. POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS* de la Guía de Gestión Integral de Riesgos en la Unidad de Gestión General (UGG), Versión 5, se acoge y establece como declaración de Política para la aplicabilidad el SIGRIP.

## 2.4 Apoyo para la implementación del SIGRIP

La adecuada implementación del SIGRIP en la UGG requiere del compromiso y participación de acuerdo con los roles y responsabilidad anteriormente descrito, contribuyendo a la identificación y ejecución de atributos comportamentales que se requieren, dispuestos a través de una estrategia de formación, comunicación, y documentación de cada una de las actividades que se ejecuten en el marco del sistema, entre ellas las siguientes:

- Identificar los recursos financieros y humanos, soluciones de TI, habilidades especializadas, infraestructura organizacional, material de referencia y experiencia que dispone.

- Establecer requisitos de educación, formación y experiencia apropiados para la implementación del sistema

- Asegurar la toma de conciencia del personal, los líderes, el administrador, la Alta Dirección y, en general, de toda la entidad, sobre el Sistema de Gestión de Riesgos para la Integridad Pública

– SIGRIP. En esa medida, se debe asegurar incluir dentro de la acción de Formación del Programa de Transparencia y Ética Pública la toma de conciencia sobre:

  - Los objetivos y alcance del Sistema
  - Cada uno se sus elementos
  - Los beneficios que tiene el Sistema para la organización
  - Las implicaciones del incumplimiento de los requisitos del Sistema

- Comunicar interna y externamente los resultados de su operación, así como cualquier actualización del Sistema o de algunos de sus elementos.

- Cada uno de los elementos del Sistema debe estar correctamente documentado. En consecuencia, una vez se implemente, deben llevarse a cabo las gestiones necesarias para incluir en el Sistema de Gestión los documentos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, así como en la gestión archivística de la entidad.

## 2.5 Operación del SIGRIP

El Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP) se concibe como un conjunto articulado de elementos que interactúan entre sí para fortalecer la gestión de los riesgos asociados a la integridad pública en la entidad. Su elemento central está constituido por la Política de Gestión Integral de Riesgos, descrita en el numeral *4. POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS* de la Guía de Gestión Integral de Riesgos en la Unidad de Gestión General (UGG), Versión 5, la cual establece los mecanismos para la identificación, análisis y valoración de la tipología de riesgos gestionados por la entidad.

Adicionalmente, el SIGRIP se complementa con tres elementos estratégicos que fortalecen la gestión del riesgo, a saber: la debida diligencia en el conocimiento de las contrapartes, la delegación de la función de cumplimiento y las herramientas de gestión del riesgo, los

cuales se articulan de manera integral, tal como se presenta a continuación

*Figura No. 1. Sistema de Riesgos para la Integridad Pública*


*Fuente: Guía para la gestión integral del riesgo en entidades públicas V7 - Secretaría de Transparencia de la Presidencia de la República, 2025*

De acuerdo con la figura anterior, la Unidad de Gestión General (UGG) del Ministerio de Defensa desarrollará el Sistema, apalancándose en la implementación del Programa de Transparencia y Ética Pública (PTEP) adoptado por la entidad y en las actividades planificadas dentro del Plan de Ejecución y Monitoreo (PEM).

Es importante señalar que las declaraciones de política enunciadas en la sección denominada "Herramientas" se acogerán y se integrarán a la Política de Gestión Integral de Riesgos de la UGG, la cual se constituye como la única declaración de política aplicable a los Sistemas de Gestión de la entidad.

## PASO 1: IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

### 2.6 Identificación de Riesgos de Integridad Pública

El SIGRIP contempla una tipología de riesgos que deben ser identificados, gestionados y tratados por la entidad como se describen a continuación:

a. **Riesgos de 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 actual. 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.*

b. ***Riesgos de 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.*

c. ***Riesgos de inadecuada gestión del conflicto de intereses:*** *surge cuando, 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*.[2]

d. **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", abuso del poder público para obtener beneficios privados, en contravención de los principios de legalidad, transparencia y moralidad administrativa, mediante prácticas como el soborno, la colusión, el tráfico de influencias, el peculado u otras conductas corruptas que afectan el interés general.

e. **Riesgos de LA/FT/FP - Lavado de activos (LA)/Financiación del Terrorismo (FT) / Financiación de la Proliferación de Armas de Destrucción Masiva**

[2] Guía para la gestión integral del riesgo en entidades Públicas, Versión 7, Función Pública – Pag 116 - 117

**(FP):** Corresponden a los riesgos derivados de la posibilidad de que la entidad sea utilizada, directa o indirectamente, como instrumento para ocultar, transformar, transferir o administrar recursos de origen ilícito, o para canalizar o destinar recursos a personas o grupos que puedan terminar atacando instituciones estatales, destinados a la financiación del terrorismo o de la proliferación de armas de destrucción masiva, afectando la legalidad, reputación y cumplimiento normativo institucional.

Bajo este marco, en la identificación de los riesgos de Integridad Pública es fundamental considerar los puntos críticos de riesgo asociados a las actividades que ejecuta cada proceso dentro de su flujo operativo. En particular, deben priorizarse aquellas actividades que implican intercambio, entrega o recepción de recursos, bienes o servicios, dado que estas etapas suelen concentrar mayores niveles de exposición a eventos que pueden afectar la integridad en la gestión pública.

Entre algunas de las actividades que ejecuta la Unidad de Gestión General de acuerdo con el Decreto 1874 del 2021 y que constituyen puntos críticos de riesgo porque implican:

- Interacción con terceros.
- Manejo directo de recursos públicos.
- Decisiones discrecionales.
- Entrega o recepción de bienes, servicios o dinero.

Por tanto, deben ser priorizadas en la identificación de riesgos de Integridad Pública, conforme al enfoque de la Guía DAFP v7, ya que los riesgos pueden materializarse en cualquier etapa del proceso y no únicamente en la operación final.

*Tabla No. 2. Algunas Actividades orientadoras como Puntos Críticos de Riesgo*

| **ACTIVIDADES COMO PUNTOS CRÍTICOS DE RIESGO** |
|---|
| • Recepción, almacenamiento y entrega de bienes muebles (equipos, mobiliario, activos tecnológicos).<br>• Asignación y control de parque automotor, combustible y servicios de transporte.<br>• Administración y recepción de donaciones provenientes de la DIAN u otros organismos del Estado. |

- Gestión de contratos de servicios generales (aseo, vigilancia, cafetería, mantenimiento).
- Procesos de baja de bienes muebles e inmuebles y control de inventarios.
- Ordenación, validación y trámite de pagos a proveedores y contratistas.
- Gestión de transferencias de recursos del Fondo de Defensa Nacional.
- Administración del Programa Anual de Caja (PAC).
- Control contable de donaciones en dinero o bienes.
- Recaudo por Cuota de Compensación Militar y venta de activos.
- Desarrollo de procesos de compra y contratación centralizada.
- Negociaciones y suscripción de convenios y contratos con proveedores.
- Participación en convenios de cooperación industrial y social – OFFSET.
- Interacción directa con oferentes en fases precontractual y contractual.
- Trámite y pago de nómina y prestaciones sociales.
- Reconocimiento y pago de cesantías y anticipos de cesantías.
- Autorización de comisiones, licencias, incentivos y beneficios.
- Gestión de programas de capacitación y bienestar financiados con recursos públicos.
- Gestión y ejecución de programas de bienestar para miembros de la Fuerza Pública.
- Celebración de convenios con entidades públicas y privadas para beneficios en salud y bienestar.
- Administración de recursos financieros y en especie destinados a programas sociales.
- Adquisición, distribución y control de bienes estratégicos.
- Administración y seguimiento de bienes decomisados entregados al MDN.
- Gestión del Sistema de Catalogación y Estandarización OTAN.
- Procesos de adquisición y mantenimiento de bienes de alto valor.
- Adquisición e implementación de hardware, software y servicios tecnológicos.
- Administración de contratos tecnológicos y licencias.
- Recepción de productos y servicios tecnológicos contratados.

*Fuente: Elaboración Grupo de Gestión y Valor Publico, Con base en Decreto 1874 de 2021*

## 2.7 Identificación de Áreas de Impacto.

En el marco de la gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

*La **consecuencia legal** corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños. Así pues, el impacto legal surge desde el momento en que una contraparte es vinculada a procesos judiciales o administrativos sancionatorios o que busquen declarar un incumplimiento.*

*El **contagio** corresponde a la posibilidad de que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una entidad o de un individuo relacionado. El contagio se expresa cuando a partes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad. (Guía DAFP v7)*

En coherencia con lo anterior, las consecuencias legales y de contagio, para efectos de la determinación del impacto del riesgo, deben analizarse principalmente en términos de su afectación económica. Cuando el riesgo se materializa, puede generar impactos de tipo reputacional, operativo o de cumplimiento, así como comprometer la adecuada ejecución de los recursos públicos.

En este sentido, la consecuencia reputacional se configura cuando el proceso, el Director, el coordinador o el buen nombre de la Unidad de Gestión General (UGG) del Ministerio de Defensa se ve involucrado en denuncias, investigaciones o reportajes que la asocian con prácticas contrarias a la integridad, incumplimientos normativos o hechos de corrupción en general.

Por su parte, la gestión del riesgo de Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva (LA/FT/FP) se orienta a prevenir la utilización de la entidad para dar apariencia de legalidad a activos provenientes de actividades delictivas o para canalizar recursos destinados a la realización de actividades terroristas. En este marco, independientemente de la existencia de consecuencias o de la

materialización del delito, toda operación sospechosa, incluso aquella que haya sido intentada, debe ser objeto de reporte, conforme a los lineamientos normativos vigentes.

**Nota:** *La materialización del riesgo no debe confundirse con la ocurrencia del delito, falta o conducta generadora de responsabilidad fiscal. Es posible que el riesgo se haya materializado, es decir, que haya un impacto con consecuencias negativas para la entidad, incluso antes de la vinculación formal a procesos sancionatorios. También, es posible que el riesgo se materialice aun cuando la persona termine absuelta. Por lo anterior, los riesgos para la integridad no deben entenderse como tipos penales o disciplinarios, ni la materialización del riesgo implica un prejuzgamiento.*

*Toda la gestión del riesgo tiene como principales objetivos la identificación, medición, control y el monitoreo, con el propósito de prevenir, detectar y corregir. En ningún caso podrá derivar en juicios de responsabilidad o en la aplicación de sanciones. Ante un escenario de materialización de un riesgo, la respuesta institucional debe estar encaminada a asegurar la "continuidad del negocio15", es decir, a asegurar que, a pesar del impacto que hubo en los objetivos derivados del riesgo que se materializa, estos se puedan cumplir (Guía DAFP v7)*

## 2.8 Identificación de Factores de Riesgo.

De acuerdo con lo descrito en la n la Guía para la gestión integral de riesgos (V7) del DAFP, para los riesgos de LA/FT/FP, se deben considerar los factores de riesgo asociados a las transacciones u operaciones que cada proceso realiza, tanto a nivel interno como externo, en la provisión, recepción o acceso a bienes y servicios por parte de clientes, usuarios, beneficiarios o contrapartes.

Estos factores de riesgo se relacionan con la forma en que se ejecutan las operaciones, los canales de distribución utilizados y las zonas o contextos de operación, en las cuales la entidad puede verse expuesta a ser utilizada, de manera directa o indirecta, para dar apariencia de legalidad a recursos de origen ilícito o para canalizar recursos con fines ilícitos.

En este sentido, a continuación, se identifican los principales factores de riesgo que deben ser analizados para la gestión integral del riesgo de LA/FT/FP.

- **Contrapartes:** corresponden a las personas naturales o jurídicas, públicas o privadas, nacionales o internacionales, con las cuales la UGG establece relaciones administrativas, contractuales, financieras, operativas o de cooperación para el cumplimiento de sus funciones misionales, estratégicas y de apoyo.

  Incluyen, entre otras, proveedores, contratistas, beneficiarios de programas, veteranos, usuarios de servicios, entidades del Grupo Social Empresarial del Sector Defensa (GSED), entidades públicas, organismos de cooperación, donantes y aliados estratégicos, cuya naturaleza, perfil o comportamiento puede generar exposición al riesgo de LA/FT/FP.

- **Productos:** Corresponden a los bienes, servicios, beneficios, apoyos, trámites administrativos, pagos y transferencias que la UGG gestiona, administra, entrega o financia en cumplimiento de sus funciones y desarrollo de sus competencias.

  Estos productos incluyen, entre otros, pagos de nómina, pensiones y subsidios, prestación de servicios administrativos y tecnológicos, programas de bienestar, entre otros, así como bienes y servicios adquiridos mediante procesos de contratación estatal. El riesgo asociado surge de su valor, volumen, complejidad, forma de asignación o entrega, y de los controles aplicados para su gestión.

- **Canales:** Los canales corresponden a los medios, mecanismos o modalidades a través de los cuales la UGG – MDN interactúa con sus contrapartes y gestiona los productos y servicios bajo su responsabilidad.
  Comprenden canales presenciales, documentales, electrónicos, digitales, interinstitucionales y financieros, tales como plataformas de información, sistemas transaccionales, transferencias bancarias, trámites administrativos, convenios, intermediarios institucionales o mecanismos de

cooperación. El nivel de riesgo del canal está asociado al grado de trazabilidad, automatización, supervisión y control existente.

- **Jurisdicciones:** se refieren a las zonas geográficas, territorios o ámbitos de actuación, tanto a nivel nacional como internacional, en los cuales la entidad ejecuta recursos, desarrolla programas, mantiene relaciones con contrapartes o canaliza bienes y servicios.

  El riesgo vinculado a las jurisdicciones se incrementa cuando estas presentan condiciones de vulnerabilidad, como presencia de economías ilícitas, conflictos armados, debilidad institucional, fronteras sensibles o territorios catalogados de mayor riesgo, lo que puede facilitar la materialización de riesgos de LA/FT/FP.

En este sentido es importante que se realice un ejercicio de segmentación de factores de riesgo a nivel interno que permita a los procesos identificar específicamente las señales de alerta a las operaciones que se salen de la normalidad identificada y que pueden ser catalogadas como operaciones inusuales objeto de estudio por parte del proceso y de la función de cumplimiento, con el fin de efectuar los reportes oportunos a las autoridades competentes.

A su vez se puede disponer de la metodología para la gestión de riesgos generales descrita en el Anexo 3 de la Guía de Gestión Integral de Riesgos en la UGG (V5) numeral 1.3. Identificación de áreas de factores de riesgo, ejercicio que describe algunas situaciones de riesgo frente a Riesgos de Integridad Pública y que pueden ser un insumo de consulta para los procesos.

## 2.9 Descripción del Riesgo

La descripción del Riesgo se realizará de acuerdo con la metodología para la gestión de riesgos generales descrita en el Anexo 3 de la Guia de Gestión Integral de Riesgos en la UGG (V5) numeral 1.4. Descripción del Riesgo, manteniendo la estructura de: iniciaran con "Posibilidad de" señalando el impacto, la causa inmediata y la causa raíz.

Frente a la causa inmediata de acuerdo con lo descrito en el numeral "2.6 Identificación de Riesgos de Integridad Pública" estas podrán ser el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP.

*Tabla No. 3. Ejemplo descripción de riesgo de integridad pública*

| Impacto | Causa Inmediata | | Causa Raíz |
|---|---|---|---|
| Afectación económica y/o reputacional | Fraude Interno | Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. | Descripción de la actividad en el flujo del proceso |
| 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 actúe o se abstenga de actuar…() | Descripción de la actividad en el flujo del proceso |
| 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: Guía para la gestión integral del riesgo en entidades públicas V7 - Secretaría de Transparencia de la Presidencia de la República, 2025*

Aplicando la estructura defina la descripción de los riesgos deben tener la siguiente redacción:

- Posibilidad de afectación económica por Fraude Interno en la asignación de subsidios a causa de errores, omisiones, informes

inexactos o descripciones incorrectas realizados para beneficio personal o de terceros en la asignación de subsidios

- Posibilidad de afectación reputacional por Soborno Entrante al aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.

- Posibilidad de afectación reputacional por Soborno Saliente en el seguimiento a la agenda legislativa de la Entidad, a causa del ofrecimiento indebido de incentivos o recompensas para que una persona actúe o se abstenga de actuar en favor de la entidad

- Posibilidad de afectación económica por conflicto de interés no declarado y/o declarado, pero no gestionado y/o declarado y no aceptado, a causa de decisiones en asuntos sobre los cuales la servidora o servidor público tiene un interés particular en desarrollo del comité de contratación.

- Posibilidad de afectación económica por Corrupción en la evaluación en la evaluación de los procesos de selección para la contratación de bienes y servicios de la Entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico.

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 a continuación:

*Tabla No. 4. Ejemplo de acuerdo con estructura.*

| Impacto | Causa Inmediata | Causa Raíz |
|---|---|---|
| Afectación económica, 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: Guía para la gestión integral del riesgo en entidades públicas V7 - Secretaría de Transparencia de la Presidencia de la República, 2025*

- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas en las operaciones de pago de subsidios

- Posibilidad de contagio por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de contratación directa.

- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de recaudo.

**Paso 2: Análisis y Valoración del Riesgo**: se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

- Probabilidad: se determina según el número de veces que se pasa por el punto de riesgo.
- Impacto: considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico.
- Matriz de Calor: zona de riesgo inicial (Extremo, Alto, Moderado o Bajo).

**Paso 3: Diseño y Evaluación de Controles**: se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

- Tipos de Control: Pueden ser preventivos, detectivos o correctivos.
- Atributos: Responsable, acción, complemento

**Paso 4: Valoración De Riesgo Residual:** se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

**Paso 5: Tratamiento del Riesgo:** se realizará de acuerdo con lo establecido en el Anexo 3 "METODOLOGÍA GENERAL PARA LA GESTIÓN DE RIESGOS".

| | |
|---|---|
| **Elaborado por:** | ***TE. Maira Gimena Botina Benavides*** |
| **Cargo:** | ***Asesora Grupo de Gestión y Valor Público*** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |
| **Revisado por:** | **CT. Monica Soraya Castillo Gonzalez** |
| **Cargo:** | **Coordinadora Grupo de Gestión y Valor Público** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |
| **Aprobado por:** | ***Gloria Stefany Cuesta Andrade*** |
| **Cargo:** | ***Directora de Planeación y Presupuesto*** |
| **Firma:** | ***Original debidamente firmado reposa en archivo carpeta digital del Grupo Gestión y Valor Público*** |